European Cloud Service
Data Protection Certification

AUDITOR-Konformitätsbewertungs-Programm

- Fassung 0.99b -

Stand 28.09.2020

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Kriterienkatalog
- Ermittlungsmethoden
- Modularitätskonzept
- Schutzklassenkonzept
- DIN SPEC 27557

Online verfügbar: www.auditor-cert.de

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Energie gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Autoren

Ali Sunyaev[a], Alexander Roßnagel[b], Sebastian Lins[a], Natalie Maier-Reinhardt[b], Heiner Teigeler[a]

[a] Forschungsgruppe Critical Information Infrastructures am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

[b] Projektgruppe verfassungsverträglichen Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
AUDITOR	European Cloud Service Data Protection Certification (Bezeichnung des Forschungsprojekts)
BDSG	Bundesdatenschutzgesetz
DAkkS	Deutsche Akkreditierungsstelle GmbH
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
DSK	Datenschutzkonferenz
i.S.d.	Im Sinne des
IaaS	Infrastucture as a Service
Lit.	Litera
Nr.	Nummer
PaaS	Platform as a Service
s.	siehe
SaaS	Software as a Service
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen im AUDITOR-Konformitätsbewertungsprogramm sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z.B. ist bei der Bezeichnung *Evaluator* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

1 Einleitung

1.1 Funktion und Ziele des AUDITOR-Konformitätsbewertungsprogramm

Die AUDITOR-Zertifizierung liefert einen Nachweis über die Konformität von Datenverarbeitungsvorgängen von Cloud-Anbietern mit den Anforderungen der EU-Datenschutzgrundverordnung (DSGVO). Gemäß Art. 43 Abs. 1 Satz 1 DSGVO können Zertifizierungsstellen neben Datenschutz-Aufsichtsbehörden Zertifizierungen erteilen. Eine Zertifizierungsstelle darf ihre Tätigkeit jedoch nur aufnehmen, wenn sie durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) in Zusammenarbeit mit der zuständigen Datenschutz-Aufsichtsbehörde akkreditiert wurde. Voraussetzung der Akkreditierung ist die Einhaltung der Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der Datenschutzkonferenz (DSK) zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065.

Maßgeblich für die Akkreditierung ist ein Konformitätsbewertungsprogramm, das für jedes Zertifizierungsverfahren erstellt werden muss. Das Konformitätsbewertungsprogramm beschreibt die spezifischen Anforderungen, Regeln sowie Prüfverfahren, die zur Konformitätsbewertung von Datenverarbeitungsvorgängen verwendet werden müssen, um die mit der Zertifizierung verbundene Aussage, auf wissenschaftlich rückführbare und systematische Weise treffen zu können (s. DAkkS 71 SD 0 016). Das vorliegende *‚AUDITOR-Konformitätsbewertungsprogramm‘* beschreibt daher die von der Zertifizierungsstelle zu erfüllenden Grundsätze und umfasst im Wesentlichen Anforderungen an die Zertifizierungsstelle und den Zertifizierungsprozess. Das AUDITOR-Konformitätsbewertungsprogramm wird durch das Kompetenznetzwerk Trusted Cloud e.V. als Programmeigner verwaltet und weiterentwickelt. Es wird interessierten Zertifizierungsstellen zu nicht-diskriminierenden Bedingungen zur Verfügung gestellt, um eine breite Anwendung des Zertifizierungsverfahrens sicherzustellen.

1.2 Fortentwicklung vom TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte Trusted Cloud Datenschutz-Profil (TCDP) untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. ISO 27701 – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.5.2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies geschieht mit dem *‚AUDITOR-Kriterienkatalog‘*, welcher alle relevanten Vorschriften für die Datenschutz-Zertifizierung von Cloud-Diensten in der Datenschutz-Grundverordnung fokussiert und diese zu prüffähigen Kriterien konkretisiert.

Im Rahmen des Pilotprojekts wurde auch eine Verfahrensordnung für Zertifizierungen nach dem TCDP erstellt. Eine Akkreditierung dieser Verfahrensordnung wurde jedoch nicht vorgenommen. Diese Verfahrensordnung wurde bei der Entwicklung des AUDITOR-Konformitätsbewertungsprogramms berücksichtigt. Eine Anpassung der TCDP-Verfahrensordnung ist in Hinblick auf die Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065 erforderlich und wird durch das AUDITOR-Konformitätsbewertungsprogramm adressiert.

1.3 Aufbau und Inhalte des Konformitätsbewertungsprogramms

Das AUDITOR-Konformitätsbewertungsprogramm gliedert sich in vier wesentliche Kapitel. In Kapitel 2 werden der Zweck des Konformitätsbewertungsprogramms festgelegt und zentrale Begriffe definiert. Kapitel 3 regelt die Grundsätze zur Durchführung von Zertifizierungstätigkeiten, um unter anderem Vertrauen in die Zertifizierungstätigkeiten und Ergebnisse zu schaffen. Kapitel 4 legt Anforderungen an die Zertifizierungsstelle fest, darunter bspw. Anforderungen an Struktur und Ressourcen der Zertifizierungsstelle. Kapitel 5 beschreibt Anforderungen an den Zertifizierungsprozess, aufgegliedert in die Prozessphasen Auswahl, Ermittlung, Bewertung, Entscheidung, Bestätigung und Überwachung.

Bei der Spezifikation eines Konformitätsbewertungsprogramms ist die Festlegung der Prüfung der einzelnen Kriterien wesentlich, um sicherzustellen, dass verschiedene Prüfer zum gleichen Ergebnis der Konformitätsbewertung kommen. Aus diesem Grund wird pro Kriterium im Begleitdokument *‚AUDITOR-Ermittlungsmethoden‘* angegeben, wie das jeweilige Kriterium zu prüfen ist.

2 Grundlagen

2.1 Das AUDITOR-Konformitätsbewertungsprogramm

§ 2.1.1 Bezeichnung des Konformitätsbewertungsprogramms

(1) Die Bezeichnung dieses Programms lautet: AUDITOR-Konformitätsbewertungsprogramm.
(2) Der Name der Zertifizierung wird zurzeit abgestimmt. Es wird ein Markenschutz auf europäischer Ebene angestrebt. Der Programmeigner informiert die DAkkS über die finale Festlegung des Namens.

§ 2.1.2 Zweck des Konformitätsbewertungsprogramms

(1) Ziel der AUDITOR-Zertifizierung ist es Vertrauen in die Datenverarbeitung von Cloud-Diensten bei der Verarbeitung von personenbezogenen Daten zu schaffen.
(2) Die AUDITOR-Zertifizierung liefert einen Nachweis über die Konformität von Datenverarbeitungsvorgängen von Cloud-Anbietern mit den Anforderungen der Datenschutz-Grundverordnung.
(3) Dieses Konformitätsbewertungsprogramm legt Anforderungen an die Zertifizierungsstelle und die Durchführung des Zertifizierungsprozesses fest, deren Einhaltung sicherstellen soll, dass das AUDITOR-Zertifizierungsverfahren durch die Zertifizierungsstellen kompetent, konsequent und unparteiisch betrieben wird.
(4) Durch dieses Konformitätsbewertungsprogramm soll zudem sichergestellt sein, dass die Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065 eingehalten werden.

§ 2.1.3 Konformitätsbewertungsart

(1) Dieses Konformitätsbewertungsprogramm unterfällt der Konformitätsbewertungsart „Zertifizierung“ im Sinne der ISO/IEC 17065:2012.
(2) Dieses Programm fällt im Sinne der ISO/IEC 17067:2013 Tz. 5.3.8 unter den Programmtyp 6.

§ 2.1.4 Programmeigner

(1) Der Programmeigner ist eine Person oder Organisation, die für die Entwicklung und Aufrechterhaltung dieses Konformitätsbewertungsprogramms verantwortlich ist (s. ISO/IEC 17065:2012 Tz. 3.11). Der Programmeigner vereinbart und überwacht durch eine rechtlich bindende Vereinbarung mit akkreditierten Zertifizierungsstellen, die Einhaltung der Zertifizierungsanforderungen zur Vergabe von Konformitätszeichen (s. DAkkS 71 SD 0 016).
(2) Der Programmeigner dieses Konformitätsbewertungsprogram ist das Kompetenznetzwerk Trusted Cloud e.V. Beim Kompetenznetzwerk Trusted Cloud e.V. ist ein Beirat zur Durchführung, der Leitung und Lenkung dieses Programms eingerichtet (s. ISO/IEC 17067:2013 Tz. 6.3.5). Der Beirat stellt das Beschlussorgan über

   (a) Änderungen/Ergänzungen des AUDITOR-Kriterienkatalogs,
   (b) Änderungen des AUDITOR-Konformitätsbewertungsprogramms,
   (c) Fragen der Internationalisierung und Standardisierung, und
   (d) bei Kooperationen dar,

(3) und nimmt eine beratende Funktion bei allen Fragen der Marktansprache und Lizensierung der Zertifizierung ein. Der Beirat setzt sich aus Folgenden Vertretern zusammen:

   (a) 2 Vertreter des Karlsruhe Institute of Technology (geplant: Prof. Sunyaev; Herr Lins)
   (b) 2 Vertreter der Universität Kassel (geplant: Prof. Roßnagel, Prof. Hornung)
   (c) 2 Vertreter des Bundesministeriums für Wirtschaft und Energie (geplant: Dr. Tettenborn; Dr. Werner)
   (d) 1 Vertreter des Bundeministerium des Innern (noch zu benennen)
   (e) 1 Vertreter des Kompetenznetzwerks Trusted Cloud e.V. (geplant: Herr Niessen)

   Konsultativ können weitere Experten aus Wirtschaft, Politik und Wissenschaft hinzugezogen werden; dies betrifft u.a. die Mitglieder des heutigen Lenkungsausschusses und Expertenbeirats des AUDITOR-Forschungsprojekts (u.a. Bitkom, Stiftung Datenschutz, BfDI).
(4) Der Programmeigner übernimmt die volle Verantwortung für die Ziele, den Inhalt und die Vollständigkeit dieses Programms (s. ISO/IEC 17067:2013 Tz. 6.3.4).

(5) Der Programmeigner pflegt dieses Programm und gibt bei Bedarf Anleitung für Zertifizierungsstellen (s. ISO/IEC 17067:2013 Tz. 6.3.5). Dazu werden folgende Aktivitäten ausgeführt:

(a) Durchführung von Änderungen an den festgelegten Zertifizierungskriterien (s. ISO/IEC 17067:2013 Tz. 6.6.2);
(b) Leitung der Standardisierungsaktivitäten der Zertifizierungskriterien (bspw. Überführung in DIN-, EU- oder ISO-Norm).;
(c) Durchführung von Änderungen an diesem Konformitätsbewertungsprogramm;
(d) Beobachtung von
    (i) Änderungen der rechtlichen Rahmenbedingungen, die sich durch Gesetzesnovellierungen, den Erlass delegierter Rechtsakte der Europäischen Kommission, Entscheidungen des Europäischen Datenschutzausschusses und Gerichtsentscheidungen ergeben;
    (ii) Fortentwicklungen des Stands der Technik;
    (iii) Änderungen von Anforderungen der Datenschutz-Aufsichtsbehörde und des Datenschutzausschusses an Kriterienkatalogen und Zertifizierungsverfahren;
    (iv) Rechtsakten und anderen Vorgaben von dem Datenschutzausschuss oder Datenschutz-Aufsichtsbehörden.
(e) Informieren der akkreditierten Zertifizierungsstellen bei relevanten bzw. wesentlichen Änderungen;
(f) Koordination von Kooperationen mit Interessengruppen zur Pflege und Weiterentwicklung des Programms und der Zertifizierungskriterien;
(g) Durchführung und Koordination von Tätigkeiten zur Internationalisierung der Zertifizierung, bspw. Einreichung als Europäischen Datenschutzsiegel beim EU-Ausschuss;
(h) Beratende Aktivitäten bei allen Fragen der Marktansprache;
(i) Informationsaustausch und Abstimmung mit der DAkkS, DSK, AK Zertifizierung und nationalen Datenschutz-Aufsichtsbehörden.

(6) Der Programmeigner schätzt die Risiken/Verbindlichkeiten, die aus seinen Tätigkeiten entstehen, ein und handhabt diese entsprechend (s. ISO/IEC 17067:2013 Tz. 6.3.10).
(7) Der Programmeigner stellt sicher, dass Informationen über dieses Programm der Öffentlichkeit zugänglich gemacht werden, um Transparenz, Verständnis und Akzeptanz sicherzustellen (s. ISO/IEC 17067:2013 Tz. 6.4.5). Hierzu werden folgende Maßnahmen durchgeführt:

(a) Veröffentlichung der Zertifizierungskriterien im AUDITOR-Kriterienkatalog mit freiem Zugang für alle Interessengruppen auf dem Internetportal der Zertifizierung;
(b) Weitergabe dieses Programms an Cloud-Anbieter, Datenschutz-Aufsichtsbehörde, Zertifizierungsstellen und bei Bedarf an weitere Interessengruppen durch elektronische Übermittlung des Programms.

§ 2.1.5 Anwendungsbereich

(1) Dieses Konformitätsbewertungsprogramm enthält Zertifizierungsanforderungen an die Kompetenz, die einheitliche Arbeitsweise und die Unparteilichkeit von Zertifizierungsstellen für die Datenschutzzertifizierung von Datenverarbeitungsvorgängen in Cloud-Diensten gemäß den Anforderungen der Datenschutz-Grundverordnung.
(2) Die Zertifizierung nach AUDITOR steht allen privatwirtschaftlichen Cloud-Anbietern offen, die als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO agieren und die Konformität ihrer Datenverarbeitungsvorgänge mit der Datenschutz-Grundverordnung nachweisen wollen.
(3) Die Zertifizierungskriterien werden in der maßgeblichen Fassung des AUDITOR-Kriterienkatalog festgelegt.
(4) Das Konformitätsbewertungsprogramm wird interessierten Zertifizierungsstellen zu nicht-diskriminierenden Bedingungen zur Verfügung gestellt, um eine Akkreditierung nach diesem Programm zu ermöglichen und eine breite Anwendung des Zertifizierungsverfahrens sicherzustellen.

§ 2.1.6 Änderungen an diesem Konformitätsbewertungsprogramm

(1) Änderungen an diesem Konformitätsbewertungsprogramm werden durch den Programmeigner durchgeführt.
(2) Der Programmeigner verpflichtet sich, zukünftige Änderungen des Programms über geeignete Kommunikationskanäle den akkreditierten Zertifizierungsstellen, nach diesem Programm zertifizierten Cloud-Anbietern, Datenschutz-Aufsichtsbehörde und der DAkkS sowie

bei Bedarf weiteren Interessengruppen frühzeitig mittzuteilen. Wurden die Änderungen genehmigt (i.d.R. durch die DAkkS und zuständige Datenschutzaufsichtsbehörde) werden die akkreditierten Zertifizierungsstellen und zertifizierten Cloud-Anbieter ebenfalls zeitnah informiert.

§ 2.1.7 Entwicklungshistorie

(1) Das Konformitätsbewertungsprogramm wurde im Rahmen des Forschungsprojekts AUDITOR durch die Forschungsgruppe Critical Information Infrastructures von Prof. Dr. Ali Sunyaev und den Mitarbeitern Sebastian Lins und Heiner Teigeler an dem Karlsruher Institut für Technologie und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Prof. Dr. Alexander Roßnagel und der Mitarbeiterin Dr. Natalie Maier-Reinhardt an der Universität Kassel entwickelt.

(2) Weitere Parteien wirkten an der Überarbeitung und Ausgestaltung dieses Programms mit, darunter:

(a) CLOUD&HEAT Technologies GmbH;
(b) datenschutz cert GmbH;
(c) DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN e.V.;
(d) ecsec GmbH;
(e) EuroCloud Deutschland_eco e.V., eco – Verband der Internetwirtschaft e.V.;
(f) Kompetenznetzwerk Trusted Cloud e.V.;
(g) sowie weitere assoziierte Partner des Projektes.

2.2 Begrifflichkeiten

§ 2.2.1 Zertifizierungsstelle

(1) Die Zertifizierung nach AUDITOR erfolgt durch eine unabhängige und fachlich geeignete Zertifizierungsstelle, welche im Sinne einer Konformitätsbewertungsstelle als dritte Seite auftritt (s. ISO/IEC 17000:2004 Tz. 2.5, DSK Tz. 4.2.1).

(2) Die Zertifizierungsstelle muss eine rechtsfähige Organisation oder ein abgegrenzter Teil einer rechtsfähigen Organisation sein. Gemäß Artikel R 17 Abs. 3 S. 1 des Beschlusses Nr. 768/2008/EG muss es sich bei einer Zertifizierungsstelle um einen unabhängigen Dritten handeln, der mit der Einrichtung, die er bewertet, in keinerlei Verbindung steht (s. DSK Tz. 4.2.1).

(3) Die Zertifizierungsstelle führt ihre Tätigkeit nicht-diskriminierend, vertraulich und unparteilich aus.

(4) Zertifizierungsstellen müssen sich nach der ISO/IEC 17065 i.V.m. den ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DSGVO und diesem Programm akkreditieren lassen, um damit die Erfüllung der Zertifizierungsanforderungen, insbesondere die Erfüllung der Grundsätze, nachzuweisen.

(5) Die Zertifizierungsstelle steht in einem Vertragsverhältnis mit dem zu zertifizierenden Cloud-Anbieter und ggf. zu ausgegliederten Evaluatoren.

§ 2.2.2 Evaluierung

(1) Evaluierung bezeichnet die Konformitätsbewertungsfunktionen Auswahl und Ermittlung (s. ISO/IEC 17065:2012 Tz. 3.3).

§ 2.2.3 Evaluatoren

(1) Evaluatoren im Sinne dieses Programms sind natürliche Personen, die der Zertifizierungsstelle angehören und die Auswahl- und/oder Ermittlungstätigkeiten nach diesem Programm durchführen.

(2) Eine Zertifizierungsstelle kann zudem eine ausgegliederte, unabhängige und fachlich kompetente Prüfstelle oder (einzelne) externe Evaluatoren zur Durchführung der Auswahl- und/oder Ermittlungstätigkeiten gemäß ISO/IEC 17065:2012 Tz. 6.2.2 benennen (s. § 4.2.5). Mittarbeiter dieser Prüfstellen und externe Evaluatoren werden entsprechend als ausgegliederte Evaluatoren bezeichnet. Sie führen ihre Tätigkeit nichtdiskriminierend, vertraulich und unparteilich aus.

(3) Prüfstellen und ausgegliederte Evaluatoren haben ein Vertragsverhältnis mit der Zertifizierungsstelle. Ein Vertragsverhältnis darf nicht mit einem zu zertifizierenden Cloud-Anbieter bestehen (s. § 4.2.5).

§ 2.2.4 Entscheider

(1) Entscheider im Sinne dieses Programms sind natürliche Personen, die der Zertifizierungsstelle angehören und die die Bewertung und/oder die Entscheidung über die Zertifizierung und/oder anschließend die Genehmigung der Zertifizierung durchführen.

§ 2.2.5 Akkreditierungsstelle

(1) Eine Akkreditierungsstelle ist eine befugte Stelle, die Akkreditierungen durchführt (s. ISO/IEC 17000:2004 Tz. 2.6).
(2) Eine Akkreditierung ist eine Bestätigung durch eine dritte Seite, die formal darlegt, dass eine Konformitätsbewertungsstelle (hier Zertifizierungsstelle) die Kompetenz besitzt, bestimmte Konformitätsbewertungsaufgaben (hier Zertifizierung) durchzuführen (s. ISO/IEC 17000:2004 Tz. 5.6).
(3) In Deutschland ist die DAkkS alleinig zuständig für die Durchführung von Akkreditierungen.

§ 2.2.6 Gegenstand der Bewertung/Zertifizierungsgegenstand

(1) Gegenstand der Bewertung (i.S.d. Tz. A.2.2 ISO/IEC 17000:2004, Anhang A) sind Datenverarbeitungsvorgänge mit personenbezogenen Daten i.S.d. Art. 4 Nr. 1 DSGVO, die in Cloud-Diensten oder mit Hilfe von (auch mehreren) Cloud-Diensten erbracht werden.
(2) Das Begleitdokument *‚AUDITOR-Zertifizierungsgegenstand‘* zu diesem Programm enthält eine detaillierte Herleitung und Beschreibung des Zertifizierungsgegenstandes. Zertifizierungsstellen und (ausgegliederte) Evaluatoren müssen sich mit diesem Begleitdokument vertraut machen.

§ 2.2.7 Cloud-Dienste

(1) Cloud-Dienste im Sinne dieses Konformitätsbewertungsprogramms sind Cloud-Dienste gemäß der Definition des National Institute of Standards and Technology (NIST) (2011).
(2) Cloud-Dienste ermöglichen einen flexiblen und bedarfsorientierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen, die jederzeit und überall über das Internet oder ein Netzwerk abgerufen werden können.
(3) Die für Cloud-Dienste kennzeichnenden Charakteristiken sind der bedarfsgerechte Zugriff, eine Netzwerkanbindung, die Möglichkeit zur Ressourcenbündelung, eine hohe Skalierbarkeit und eine verbrauchsabhängige Bezahlung:

   (a) Bedarfsgerechter Zugriff: Der bedarfsgerechte Zugriff ermöglicht es Cloud-Nutzern selbstständig und nahezu unmittelbar Leistungsparameter der in Anspruch genommenen Cloud-Dienste anzupassen. Dies kann insbesondere automatisch und ohne menschliche Interaktion mit den jeweiligen Cloud-Anbietern durchgeführt werden.
   (b) Netzwerkanbindung: Cloud-Dienste werden über ein Breitbandnetzwerk bereitgestellt, in der Regel über das Internet.
   (c) Skalierbarkeit: Bereitgestellte Ressourcen können flexibel und schnell, in einigen Fällen vollautomatisch, erhöht oder freigegeben werden, um so die Ressourcen auf den aktuellen Bedarf abzustimmen.
   (d) Verbrauchsabhängige Bezahlung: Um Cloud-Dienste messbar und transparent zu gestalten, kontrollieren und optimieren Cloud-Dienste den Ressourcenverbrauch anhand von service-abhängigen Kennzahlen, bspw. dem Speicherplatz, der Rechenleistung oder der Bandbreite. Dadurch kann eine bedarfsgerechte Abrechnung angeboten und durchgeführt werden. Zudem wird die Ressourcennutzung überwacht, kontrolliert, protokolliert und kommuniziert, sodass sowohl für die Cloud-Nutzer als auch für den Cloud-Anbieter, Transparenz über die Nutzung geschaffen wird.

(4) Im Rahmen dieses Konformitätsbewertungsprogramms wird zwischen den drei grundlegenden Dienstmodellen Software as a Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS) unterschieden. Darüber hinaus finden sich in der Praxis und Literatur eine Vielzahl von weiteren Dienstmodellen, bspw. Database as a Service oder Security as a Service. Allerdings lassen sich diese spezifischen Dienstmodelle im Allgemeinen den grundlegenden Modellen Infrastructure, PaaS und SaaS zuordnen.

   (a) SaaS. Der Cloud-Nutzer kann mittels verschiedener Geräte entweder über ein Thin-Client-Interface, bspw. einen Web-Browser, oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen.

(b) PaaS. Der Cloud-Nutzer kann selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Anbieters installieren und betreiben. Hierzu werden Betriebssysteme, Datenbanken, Programmierumgebungen, Programmbibliotheken oder weitere vom Cloud-Anbieter unterstützte Dienste und Werkzeuge genutzt.

(c) IaaS. Der Cloud-Nutzer erhält Zugang zu Hardwareressourcen des Cloud-Anbieters, darunter fallen bspw. Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger Software verwenden, bspw. Betriebssysteme oder Anwendungen.

(5) Cloud-Dienste können ferner Bestandteil von anderen Cloud-Diensten sein, sodass in der Praxis vermehrt verschachtelte Wertschöpfungsketten oder -netzwerke von Cloud-Diensten auftreten. Die Verantwortlichkeiten des Cloud-Dienstes und die Abhängigkeiten und Schnittstellen zu anderen Cloud-Diensten sind im Rahmen der Zertifizierung daher klar zu benennen und abzugrenzen.

(6) Cloud-Dienste sind Dienstleistungen im Sinne der ISO/IEC 17065:2012.

(7) Das Begleitdokument *‚AUDITOR-Zertifizierungsgegenstand*‘ zu diesem Programm enthält eine detaillierte Beschreibung von Cloud-Diensten in Bezug auf den Zertifizierungsgegenstand.

§ 2.2.8 Datenverarbeitungsvorgänge in Cloud-Diensten

(1) Eine Datenverarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

(2) Ein Datenverarbeitungsvorgang kann sowohl technische und automatisierte als auch nichttechnische und somit auch organisatorische (bspw. manuelle oder personelle) Vorgangsschritte enthalten, worunter auch Datenschutzkonzepte und -managementsysteme fallen können.

(3) Der gesamte Verarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

(4) Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können.

(5) Die Eignung eines Datenverarbeitungsvorgangs für die AUDITOR-Zertifizierung wird im Rahmen der Auswahltätigkeiten überprüft (s. 5.1).

(6) Das Begleitdokument *‚AUDITOR-Zertifizierungsgegenstand‘* zu diesem Programm enthält eine detaillierte Beschreibung von Datenverarbeitungsvorgängen in Cloud-Diensten in Bezug auf den Zertifizierungsgegenstand.

§ 2.2.9 Cloud-Anbieter

(1) Cloud-Anbieter sind Rechtsträger, die Cloud-Dienste betreiben.

(2) Cloud-Anbieter stellen die Kunden der Zertifizierungsstelle dar.

(3) Cloud-Anbieter sind gegenüber einer Zertifizierungsstelle verantwortlich dafür, sicherzustellen, dass die Zertifizierungskriterien erfüllt sind (s. ISO/IEC 17065:2012 Tz. 3.1).

§ 2.2.10 Subauftragsverarbeiter

(1) Ein Cloud-Anbieter kann im Rahmen seiner Datenverarbeitungsvorgänge weitere Subauftragsverarbeiter einbeziehen, die externe Ressourcen und Dienstleistungen für die Durchführung der Datenverarbeitungsvorgänge bereitstellen.

(2) Subauftragsverarbeiter sind Rechtsträger, die Produkte oder Dienstleistungen betreiben, welche relevant für die zu zertifizierenden Datenverarbeitungsvorgänge sind.

(3) Ein Subauftragsverarbeiter ist unabhängig von dem Cloud-Anbieter.

(4) Setzen die zu zertifizierenden Verarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Cloud-Anbieter sonstige Subauftragsverarbeiter ein, so kann sich die Zertifizierung nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Cloud-Anbieters stehen.

Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Dienstes einsetzen.

§ 2.2.11 Cloud-Nutzer

(1) Cloud-Nutzer im Sinne dieses Programms ist jede natürliche und juristische Person, die als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO Verarbeitungen personenbezogener Daten durchführt und allein oder gemeinsam mit anderen über Zwecke und Mittel dieser Verarbeitungen entscheidet und sich entschließt, diese Verarbeitungen an einen Cloud-Anbieter auszulagern.
(2) Cloud-Nutzer stellen somit die Kunden des Cloud-Anbieters dar.

§ 2.2.12 Datenschutz-Aufsichtsbehörde

(1) Eine Datenschutz-Aufsichtsbehörde ist eine von einem Mitgliedstaat gemäß Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle (s. Art. 4 Abs. 21 DSGVO).
(2) Als zuständige Datenschutz-Aufsichtsbehörde wird eine Datenschutz-Aufsichtsbehörde bezeichnet, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

   (a) der Cloud-Nutzer als Verantwortlicher oder der Cloud-Anbieter als Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Datenschutz-Aufsichtsbehörde niedergelassen ist,
   (b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Datenschutz-Aufsichtsbehörde hat oder haben kann oder,
   (c) eine Beschwerde bei dieser Datenschutz-Aufsichtsbehörde eingereicht wurde (s. Art. 4 Abs. 22 DSGVO).

(3) Die DAkkS akkreditiert als Akkreditierungsstelle die Zertifizierungsstellen gemeinsam mit der zuständigen Datenschutzaufsichtsbehörde. Die zuständige Datenschutzaufsichtsbehörde erteilt der Zertifizierungsstelle in einem eigenständigen Verfahren auf Grundlage dieser gemeinsamen Akkreditierung die Befugnis als solche tätig werden zu dürfen (s. DSK ‚Vorwort').

§ 2.2.13 Europäischer Datenschutzausschuss

(1) Der Europäische Datenschutzausschuss wurde als Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit eingerichtet und besteht aus dem Leiter einer Datenschutz-Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern (s. Art. 68 Abs. 1 und 3 DSGVO).
(2) Der Europäische Datenschutzausschuss kann die Zertifizierungskriterien genehmigen, sodass dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führt.

§ 2.2.14 Zertifizierungskriterien

(1) Zertifizierungskriterien sind die im AUDITOR-Kriterienkatalog festgelegten normativen Anforderungen, die durch den Cloud-Anbieter als Bedingung zur Feststellung oder Aufrechterhaltung der Zertifizierung erfüllt sein müssen.
(2) Die genehmigten Kriterien werden im Sinne des Art. 42 Abs. 5 DSGVO unter Angabe des jeweiligen Verwendungszeitraums durch den Programmeigner in einer elektronischen Form veröffentlicht (s. DSK Tz. 4.6, EDPB Annex 1 Tz. 4.6).

§ 2.2.15 Zertifizierungsanforderungen

(1) Anforderungen an die Zertifizierungsstelle und das Zertifizierungsverfahren, welche durch dieses Konformitätsbewertungsprogramm vorgegeben sind.

§ 2.2.16 Schutzklassen

(1) Der AUDITOR-Kriterienkatalog nimmt bei einigen Kriterien eine Unterscheidung nach Schutzklassen vor und legt für diese unterschiedliche Zertifizierungskriterien fest, die erfüllt werden müssen. Schutzklassen stellen bei der AUDITOR-Zertifizierung ein wichtiges Instrument dar, da mit ihnen der individuelle Schutzbedarf von Datenverarbeitungsvorgängen und dessen Erfüllung durch zertifizierte Cloud-Dienste ausgedrückt werden kann.
(2) Bei der Beantragung einer Zertifizierung gibt ein Cloud-Anbieter die für seinen Cloud-Dienst entsprechende Schutzklasse an.

(3) Die Zertifizierungsstelle erstellt auf der Grundlage der Evaluierung eine Bewertung der Erfüllung der Zertifizierungskriterien des AUDITOR-Kriterienkatalogs durch die Datenverarbeitungsvorgänge in Bezug auf eine bestimmte Schutzklasse. Die Zertifizierungsstelle beurteilt jedoch nicht die Wahl der Schutzklasse. Die Schutzklasse wird allein durch den Cloud-Anbieter festgelegt und beantragt und die Zertifizierungsstelle passt entsprechend den Prüfumfang an.

(4) Das Begleitdokument *‚AUDITOR-Schutzklassenkonzept‘* zu diesem Programm enthält eine detaillierte Beschreibung zu den Grundlagen und Ausgestaltungen der Schutzklassen. Zertifizierungsstellen und (ausgegliederte) Evaluatoren müssen sich mit diesem Begleitdokument vertraut machen.

§ 2.2.17 Konformitätszeichen

(1) Geschütztes Zeichen, das von einer Zertifizierungsstelle ausgestellt wird und deutlich macht, dass ein Zertifizierungsgegenstand mit festgelegten Zertifizierungskriterien übereinstimmt (s. ISO/IEC 17030:2009 Tz. 3.1).

(2) Als AUDITOR-Konformitätszeichen werden ein Zertifikat und ein graphisches Gütesiegel vergeben (s. § 5.5.2, § 5.5.3, § 5.5.4).

§ 2.2.18 Interessierte Parteien

(1) Interessierte Parteien stellen Unternehmen, Privatpersonen, Behörden etc. dar, welche Interesse an der Mitgestaltung oder Mitwirkung der Zertifizierung haben und/oder die Zertifizierung samt ihrer Konformitätszeichen im Markt wahrnehmen.

(2) Interessierte Parteien können insbesondere sein:

(a) Cloud-Nutzer;
(b) Kunden von Cloud-Nutzern;
(c) Datenschutz-Aufsichtsbehörden;
(d) Teilnehmer im Cloud-Markt;
(e) Weitere Zertifizierungsstellen.

3 Grundsätze

Die Zertifizierungsstelle verpflichtet sich die Grundsätze zur Durchführung von Zertifizierungstätigkeiten einzuhalten, um das Vertrauen des Marktes in das AUDITOR-Zertifizierungsverfahren und die erteilten Konformitätszeichen sicherzustellen.

§ 3.1.1 Vermittlung von Vertrauen

(1) Übergeordnetes Ziel der Zertifizierung ist es, allen Beteiligten das Vertrauen zu vermitteln (s. ISO/IEC 17065:2012 Tz. A.1.1), dass Datenverarbeitungsvorgänge in Cloud-Diensten festgelegte Zertifizierungskriterien erfüllen. Der Wert der Zertifizierung ist der Grad an öffentlichem Vertrauen, der durch einen unparteiischen und kompetenten Nachweis einer dritten Stelle vermittelt wird.

(2) Die Zertifizierung soll es Cloud-Anbietern ermöglichen, gegenüber dem Markt nachzuweisen, dass ihren Datenverarbeitungsvorgängen die Erfüllung festgelegter Zertifizierungskriterien durch eine unparteiische dritte Stelle bestätigt wurde (s. ISO/IEC 17067:2013 Tz. 4.2.1).

§ 3.1.2 Unparteilichkeit

(1) Um Vertrauen in ihre Tätigkeiten und Ergebnisse zu schaffen, ist es für die Zertifizierungsstellen und ihr Personal erforderlich, unparteiisch zu sein und als unparteiisch empfunden zu werden (s. ISO/IEC 17065:2012 Tz. A.2.1).

(2) Unparteilichkeit beschreibt das Vorhandensein von Unabhängigkeit und Objektivität (s. DSK Tz. 4.2). Unabhängigkeit bedeutet, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann und deren finanzielle Stabilität sichergestellt ist (s. DSK ‚Kapitel 5'). Objektivität bedeutet, dass Interessenkonflikte nicht existieren oder beigelegt wurden, um nachfolgende Zertifizierungstätigkeiten nicht nachteilig zu beeinflussen.

(3) Die Zertifizierungsstelle muss für die Unparteilichkeit ihrer Zertifizierungstätigkeiten verantwortlich sein. Sie darf keinen kommerziellen, finanziellen oder sonstigen Druck zulassen, der die Unparteilichkeit gefährdet.

(4) Die Zertifizierungsstelle ist dafür verantwortlich sicherzustellen, dass auch ausgegliederte Evaluatoren ihre Tätigkeiten unparteiisch durchführen und die Anforderungen zur Unparteilichkeit erfüllen und fortlaufend einhalten. Insbesondere liegt im Regelfall eine unzulässige Gefährdung der Unparteilichkeit vor, wenn Vertragsbeziehungen zwischen zu zertifizierenden Cloud-Anbietern und ausgegliederten Evaluatoren über die Durchführung von Evaluierungstätigkeiten vorliegen.

(5) Risiken für die Unparteilichkeit können Befangenheit miteinschließen, die entstehen kann durch (s. ISO/IEC 17065:2012 Tz. A.2.2):

   (a) Eigennutz (z. B. übermäßige Abhängigkeit von einem Dienstleistungsvertrag oder von den Gebühren oder Angst vor dem Verlust des Cloud-Anbieters oder davor, arbeitslos zu werden, in einem Ausmaß, das die Unparteilichkeit bei der Durchführung der Zertifizierungstätigkeiten nachteilig beeinflusst);
   (b) Selbstbewertung (z. B. Durchführen von Zertifizierungstätigkeiten, bei denen die Zertifizierungsstelle die Ergebnisse anderer Dienstleistungen, die sie bereits erbracht hat, wie z. B. Beratungsdienstleistungen, evaluiert);
   (c) Interessenvertretung (z. B. wenn eine Zertifizierungsstelle oder deren Personal zugunsten oder gegen eine bestimmte Firma agiert, die gleichzeitig ihr Kunde ist);
   (d) Übermäßige Vertrautheit, d. h. Risiken, die auf eine Zertifizierungsstelle oder deren Personal zurückzuführen sind, welche, anstatt sich um Konformitätsnachweise zu bemühen, zu vertraut oder leichtgläubig sind;
   (e) Einschüchterung (z. B. können die Zertifizierungsstelle oder deren Personal durch Risiken durch oder Angst vor einem Cloud-Anbieter oder einem anderen Beteiligten abgeschreckt werden, unparteiisch zu handeln);
   (f) Wettbewerb (z. B. zwischen dem Cloud-Anbieter und einer Vertragsperson, oder Zertifizierungsstellen am Markt).

(6) Insbesondere darf innerhalb von 24 Monaten das Personal der Zertifizierungsstelle nicht zur Bewertung von Datenverarbeitungsvorgängen oder zur Zertifizierungsentscheidung bezüglich Datenverarbeitungsvorgängen, für die es Beratung bereitgestellt hat, eingesetzt werden (s. ISO/IEC 17065:2012 Tz. 4.2.10).

(7) Die Einnahmequelle der Zertifizierungsstelle ist die Bezahlung der Zertifizierung durch den Cloud-Anbieter. Dadurch ist eine potentielle Gefährdung für die Unparteilichkeit gegeben. Die

Zertifizierungsstelle muss jedoch sicherstellen, dass die Art und Höhe der Bezahlung nicht die Unabhängigkeit und Objektivität der Zertifizierungstätigkeiten beeinflussen.

§ 3.1.3 Kompetenz

(1) Um Zertifizierungen erbringen zu können, die Vertrauen erzeugen, ist Kompetenz des Personals, unterstützt durch das Managementsystem der Zertifizierungsstelle, erforderlich (s. ISO/IEC 17065:2012 Tz. A.3).

(2) Die Zertifizierungsstelle stellt sicher, dass (ausgegliederte) Evaluatoren die notwendige Kompetenz zur Durchführung von (ausgegliederten) Tätigkeiten fortlaufend aufweisen.

§ 3.1.4 Vertraulichkeit und Offenheit

(1) Das Gleichgewicht zwischen den Zertifizierungsanforderungen, die sich auf die Vertraulichkeit und die Offenheit beziehen, hat einen Einfluss auf das Vertrauen der interessierten Parteien sowie deren Wahrnehmung über den Wert der durchgeführten Zertifizierung.

(2) Die Zertifizierungsstelle stellt sicher, dass (ausgegliederte) Evaluatoren die Tätigkeiten vertraulich durchführen.

(3) Sofern gesetzlich nicht anderweitig angeordnet, müssen insbesondere Personen, einschließlich Ausschussmitgliedern, Personal aus externen Stellen oder Personen, die im Auftrag der Zertifizierungsstelle tätig sind, alle Informationen, die sie während der Durchführung der Zertifizierungstätigkeiten erhalten oder erzeugt haben, vertraulich behandeln (s. ISO/IEC 17065:2012 Tz. 6.1.1.3).

(4) Eine Zertifizierungsstelle muss für den öffentlichen Zugang und die Offenlegung sachgemäßer und rechtzeitiger Informationen über ihre Auswahl-, Ermittlungs- und Zertifizierungsprozesse sowie über den Zertifizierungsstatus (Erteilung, Aufrechterhaltung, Erweiterung oder Einschränkung des Geltungsbereichs der Zertifizierung, Aussetzung, Widerruf oder Verweigerung der Zertifizierung) eines jeglichen Datenverarbeitungsvorgangs sorgen, um Vertrauen in die Integrität und Glaubwürdigkeit der Zertifizierung zu erzeugen (s. ISO/IEC 17065:2012 Tz. A.4.3). Offenheit ist ein Grundsatz für den Zugang zu oder die Offenlegung von entsprechenden Informationen.

§ 3.1.5 Durchführung der Zertifizierungstätigkeiten unter nicht-diskriminierenden Bedingungen

(1) Die Zertifizierungsstelle muss sicherstellen, dass grundsätzliche Regelungen und Verfahren, im Rahmen derer die Zertifizierungsstelle tätig ist, sowie ihre Verwaltung nicht-diskriminierend sind.

(2) Die Zertifizierungsstelle stellt sicher, dass Tätigkeiten durch (ausgegliederte) Evaluatoren nicht-diskriminierend durchgeführt werden.

§ 3.1.6 Abgrenzung der Verantwortlichkeiten

(1) Verantwortlich für die Erfüllung der Zertifizierungsanforderungen ist die Zertifizierungsstelle (s. ISO/IEC 17065:2012 Tz. A.6.1).

(2) Werden Tätigkeiten von ausgegliederten Evaluatoren durchgeführt, ist die Zertifizierungsstelle dafür verantwortlich, dass alle im Programm enthaltenen Zertifizierungsanforderungen von den ausgegliederten Evaluatoren erfüllt und eingehalten werden.

(3) Verantwortlich für die Erfüllung der Zertifizierungskriterien ist der Cloud-Anbieter, nicht die Zertifizierungsstelle (s. ISO/IEC 17065:2012 Tz. A.6.1).

(4) Die Zertifizierungsstelle trägt die Verantwortung dafür, ausreichend objektive Nachweise, auf denen die Zertifizierungsentscheidung basieren muss, einzuholen (s. ISO/IEC 17065:2012 Tz. A.6.2). Basierend auf einer Bewertung der Nachweise, trifft sie die Entscheidung, eine Zertifizierung zu gewähren, wenn die Konformität ausreichend nachgewiesen wird, oder eine Entscheidung, die Zertifizierung nicht zu gewähren, wenn die Konformität nicht ausreichend nachgewiesen wird.

§ 3.1.7 Offenheit für Beschwerden

(1) Die Zertifizierungsstelle ist offen für Beschwerden von Cloud-Anbietern oder interessierten Parteien (s. ISO/IEC 17065-1:2013 Tz. 4.1.2.2, 4.6, 7.13). Falls diese Beschwerden für begründet befunden werden, sollten sie darauf vertrauen können, dass diese Beschwerden zweckmäßig behandelt werden und dass angemessene Anstrengungen durch die Zertifizierungsstelle zu ihrer Klärung unternommen werden (s. § 4.3.2). Ein tatsächlicher Umgang mit

Beschwerden hat eine wichtige Bedeutung zum Schutz der Zertifizierungsstellen, ihrer Kunden und anderen Anwendern von Zertifizierungen vor Fehlern, Versäumnissen oder unvernünftigem Verhalten. Vertrauen in Zertifizierungstätigkeiten wird abgesichert, wenn Beschwerden entsprechend bearbeitet werden.

4 Anforderungen an eine Zertifizierungsstelle

4.1 Grundlegende Zertifizierungsanforderungen

§ 4.1.1 Akkreditierung der Zertifizierungsstelle

(1) Zertifizierungsstellen müssen sich nach der ISO/IEC 17065 i.V.m. den ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DSGVO und diesem Programm bei der DAkkS akkreditieren lassen.

(2) Die Zertifizierungsstelle darf Zertifizierungen nach diesem Programm nur durchführen, soweit eine gültige Akkreditierung vorliegt.

(3) Die Akkreditierung wird gemäß Art. 43 Abs. 3 DSGVO auf maximal fünf Jahre befristet (s. DSK ‚Geltungsdauer der Akkreditierung').

(4) Bei Aussetzung oder Zurückziehung der Akkreditierung (unabhängig davon, wie eine solche Entscheidung zustande gekommen ist) gelten:

(a) Die Aussetzung (temporärer Entzug der Akkreditierung) oder Zurückziehung (dauerhafter Widerruf der Akkreditierung) der Akkreditierung führt zur Ungültigkeit der vergebenen Zertifizierungen (s. DSK Tz. 4.1.2.2);

(b) Die Zertifizierungsstelle muss ihre vergebenen Zertifizierungen widerrufen, insofern diese die ausgesetzte oder zurückgezogene Akkreditierung betreffen (s. IAF/ILAC A5:11/2013 Tz. M.8.3.2.1., DSK Tz. 4.1.2.2);

(c) In der Zertifizierungsvereinbarung ist darauf hinzuweisen und verbindlich zu regeln (s. § 5.1.5), dass die Zertifizierung des Cloud-Anbieters abhängig von der Akkreditierung der Zertifizierungsstelle ist (s. DSK Tz. 4.1.2.2). Insbesondere sollen die Konsequenzen bei Aussetzung oder Zurückziehung der Akkreditierung festgehalten werden;

(d) Die Zertifizierungsstelle darf fortan keinen Gebrauch mehr von jedweder Werbung machen, die auf den akkreditierten Status Bezug nimmt.

(5) Gründe für eine Aussetzung oder Zurückziehung des Akkreditierungsbescheides durch die DAkkS können u. a. sein (s. DAkkS 71 SD 0 001 Tz. 4):

(a) Wegfall wesentlicher Akkreditierungsvorrausetzungen (z. B. Personal, Einrichtungen, Räumlichkeiten);

(b) wiederholter oder besonders schwerer Verstoß gegen Akkreditierungsregeln;

(c) bewusste Täuschung der Akkreditierungsstelle durch Übermittlung falscher oder unvollständiger Informationen, die für die Beurteilung der Zertifizierungsstelle wesentlich sind;

(d) Nichterfüllung erteilter Auflagen auch nach Stellung einer Nachfrist.

(6) Verfahren für die Handhabung der Aussetzung oder Zurückziehung der Akkreditierung sind im Management der Zertifizierungsstelle zu integrieren (s. DSK Tz. 4.1.2.2). Dazu muss die Zertifizierungsstelle insbesondere Prozesse etablieren, um:

(a) die zertifizierten Cloud-Anbieter, Cloud-Anbieter bei denen ein laufendes Zertifizierungsverfahren durchgeführt wird, Cloud-Anbieter von denen ein Zertifizierungsantrag eingereicht wurde, oder sonstige Interessengruppen die sich nach einer AUDITOR-Zertifizierung erkundigen, über die Aussetzung oder Zurückziehung der Akkreditierung sofort zu informieren und auf die Konsequenzen hinzuweisen (s. IAF/ILAC A5:11/2013 Tz. M.8.3.2.1., DSK Tz. 4.1.2.2);

(b) den Programmeigner über die Aussetzung oder Zurückziehung der Akkreditierung zu informieren, da etwaige Nutzungsrechte und -vereinbarungen mit der Zertifizierungsstelle betroffen sein können (s. Unterkapitel 4.4);

(c) jedwede Werbung (bspw. auf der Webseite) zu entfernen, die in Zusammenhang mit der Akkreditierung steht;

(d) Maßnahmen zur Wiederherstellung der Akkreditierung zu initiieren und mit der DAkkS abzustimmen;

(e) ein Transferkonzept der Zertifizierung zu erstellen und aufrecht zu erhalten (s. DSK Tz. 4.1.2.2), welches:

(i) Maßnahmen festlegt, um eine Zertifizierung innerhalb von sechs Monaten an eine aufnehmende Zertifizierungsstelle mit gültiger Akkreditierung zu überführen;

(ii) ein aktuelles und fortlaufend gepflegtes Register von akkreditierten Zertifizierungsstellen enthält, welche gemäß einer vertraglich abgeschlossenen Vereinbarung eine Zertifizierung übernehmen können;

(iii) die DAkkS bei der Begutachtung des Transfers einbezieht;
(iv) die zuständige Datenschutzaufsichtsbehörde über den Transfer informiert und diese in den Transfer auf Verlangen der Datenschutzaufsichtsbehörde einbezieht;
(v) den Programmeigner über den Transfer informiert;
(vi) in den Zertifizierungsvereinbarungen vertraglich festgehalten wird (s. § 5.1.5);
(vii) sich an den Vorgaben der IAF MD 2:2017 für die Übertragung akkreditierter Zertifizierungen von Managementsystemen orientieren kann.

(7) Eine Re-Akkreditierung in Anschluss an die Gültigkeitsdauer der Akkreditierung von fünf Jahren ist möglich, muss jedoch vor Ablauf der Gültigkeitsdauer erfolgreich abgeschlossen werden, damit bestehende Zertifizierung nicht ungültig werden.

§ 4.1.2 Vor-Ort-Begutachtung im Rahmen der Akkreditierung

(1) Im Rahmen des Akkreditierungsprozesses erfolgt eine Vor-Ort-Begutachtung durch Mitarbeiter der DAkkS und der zuständigen Datenschutzaufsichtsbehörde. Diese umfasst eine Überprüfung der in der Dokumentation der Zertifizierungsstelle beschriebenen Prozesse in ihrer praktischen Umsetzung und eine Beurteilung hinsichtlich der Akkreditierungskriterien. Ziel der Begutachtung ist die Feststellung der Kompetenz der Zertifizierungsstelle, die beantragte AUDITOR-Zertifizierung durchführen zu können sowie die Feststellung der Konformität mit allen in den Akkreditierungsregeln festgelegten Anforderungen (s. DAkkS 71 SD 0 001).
(2) Es gelten die Anforderungen gemäß den Beschreibungen in der DAkkS 71 SD 0 001 Punkt 3.2.2 und 3.2.3 sowie ggf. ergänzende Anforderungen der DAkkS im Rahmen der Begutachtung. Ferner sei auf die Beschreibung des Akkreditierungsprozesses für den Bereich „Datenschutz“ gemäß Art. 42, 43 DSGVO der DAkkS verwiesen.[1]
(3) Die Begutachtung der Zertifizierungsstelle erfolgt an deren Geschäftssitz sowie an den Orten, an denen diese Zertifizierungstätigkeiten durchführt. Seitens der Zertifizierungsstelle ist zu gewährleisten, dass Vor-Ort-Begutachtungen durch Begutachter der DAkkS bei Auftraggebern sowie ggf. bei Unterauftragnehmern dieser Zertifizierungsstelle durchgeführt werden können (s. DAkkS 71 SD 0 001). Insbesondere ist dem Begutachtungsteam Zutritt zu allen akkreditierungsrelevanten Räumlichkeiten, Aufzeichnungen und Dokumenten einschließlich Aufzeichnungen zum Personal zu gewähren, sofern dem nicht gesetzliche Regelungen entgegenstehen. Dem Begutachtungsteam ist die für seine Tätigkeit erforderliche Hilfe und Unterstützung zu gewähren, soweit dies zum Zweck der Begutachtung notwendig ist.

§ 4.1.3 Witnessing im Rahmen der Akkreditierung

(1) Um die Kompetenz der zu akkreditierenden Stelle bewerten zu können, wird im Akkreditierungsverfahren zusätzlich auf ein begleitendes Witnessing zurückgegriffen (s. DSK Tz. 6.1.2.1, ‚Anhang 2: Witnessing-Modell‘).
(2) Es gelten die Anforderungen an das Witnessing gemäß DAkkS 71 SD 0 013 Punkt 4.
(3) Das Witnessing wird durch Mitarbeiter der zuständigen Datenschutzaufsichtsbehörde (oder von der Beauftragten) und der DAkkS ausgeführt und findet grundsätzlich an dem Ort statt, an dem die Tätigkeit im Zertifizierungsprozess ausgeführt wird. Dies ist in der Regel beim Cloud-Anbieter als dem Kunden der Zertifizierungsstelle und in den Räumlichkeiten der Zertifizierungsstelle. Die DAkkS (in Abstimmung mit der zuständigen Datenschutzaufsichtsbehörde) behält sich dabei vor, festzulegen, welches Personal und welche Tätigkeiten im Zertifizierungsprozess einem Witnessing zu unterziehen sind.
(4) Der Umfang des erforderlichen Witnessing im Rahmen des Begutachtungsverfahrens wird durch die DAkkS (zusammen mit der zuständigen Datenschutzaufsichtsbehörde) nach folgenden Grundsätzen festgelegt (s. DSK ‚Anhang 2: Witnessing-Modell‘):

(a) Für die Erstakkreditierung einer Zertifizierungsstelle muss je Geltungsbereich des Konformitätsbewertungsprogramms mindestens ein Witness-Audit durchgeführt werden (s. DSK ‚Anhang 2: Witnessing-Modell‘). Da dieses Programm einen Geltungsbereich festgelegt hat (Verarbeitungsvorgänge von personenbezogenen Daten in Cloud-Diensten), erfolgt ein Witness-Audit im Rahmen der Akkreditierung nach diesem Programm;
(b) Es ist zulässig die Durchführung von ausstehenden Witness-Audits in einem angemessenen Zeitraum entsprechend ISO/IEC 17011 nachzuholen und die Akkreditierung unter Auflage der Durchführung des ausstehenden Witness-Audits zu erteilen;

[1] https://www.dakks.de/content/projekt-datenschutz

(c) Bei der anschließenden Überwachung der Akkreditierung entsprechend ISO/IEC 17011 ist für mindestens einen Anwendungsbereich aus allen Programmen der Zertifizierungsstelle ein Witness-Audit durchzuführen; im Akkreditierungszyklus müssen mindestens 50% aller Geltungsbereiche aus allen Programmen durch ein Witness-Audit abgedeckt werden;
(d) Witness-Audits dürfen in Abhängigkeit von weiteren Befunden und risikoorientierter Betrachtung jederzeit außerplanmäßig angeordnet werden.
(e) Die Anzahl an Witness-Audits kann begrenzt werden, wenn die Akkreditierungsstelle das ausreichende Vertrauen in die Arbeit der Zertifizierungsstelle begründen kann (s. DSK ‚Anhang 2: Witnessing-Modell'). Will die Zertifizierungsstelle ein neues Konformitätsbewertungsprogramm einsetzen, so ist hierfür ein erneutes Witness-Audit erforderlich.

§ 4.1.4 Sicherstellung der Unparteilichkeit

(1) Zur Sicherstellung der Unparteilichkeit gemäß § 3.1.2 muss die Zertifizierungsstelle alle Anforderungen der ISO/IEC 17065:2012 Tz. 4.2 erfüllen und fortlaufend einhalten.
(2) Die Zertifizierungsstelle muss einen Mechanismus zur Sicherung ihrer Unparteilichkeit haben. Dazu muss die Zertifizierungsstelle die Anforderungen der ISO/IEC 17065:2012 Tz. 5.2 erfüllen. Insbesondere muss eine fortlaufende Identifizierung, Dokumentation, Bewertung und Beseitigung oder Minimierung der Risiken für die Zertifizierungsstelle, deren Personal und in Beziehung stehende Stellen durchgeführt werden (s. ISO/IEC 17065 Tz. 4.2.3, 4.2.4, DAkkS 71 SD 0 013 Tz 3.1).
(3) Gemäß den Anforderungen der DSK ist Unparteilichkeit nur dann gegeben, wenn neben den Anforderungen in § 3.1.2 weiterhin die folgenden zusätzlichen Anforderungen erfüllt sind und fortlaufend eingehalten werden (s. DSK Tz. 4.2.1):

(a) Im Einklang mit Art. 43 Abs. 2 lit. a DSGVO sind der zuständigen Datenschutzaufsichtsbehörde im Rahmen des Akkreditierungsverfahrens gesonderte Nachweise über das Merkmal der Unabhängigkeit vorzulegen. Dies gilt insbesondere für die Nachweise über die Finanzierung der Zertifizierungsstelle, soweit sie die Sicherstellung der Unparteilichkeit betreffen, und Nachweise, dass Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen (s. DSK Tz. 4.2.1, ‚Kapitel 5', EDPB Annex 1 Tz. 4.2);
(b) Entsprechend Art. 43 Abs. 2 lit. e DSGVO muss die Zertifizierungsstelle der zuständigen Datenschutzaufsichtsbehörde zudem nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Solche Konflikte könnten sich z. B. durch eine hohe Umsatzabhängigkeit von Kunden oder sonstigen wirtschaftlichen Druck auf die Zertifizierungsstelle ergeben (s. DSK Tz. 4.2.1, ‚Kapitel 5', EDPB Annex 1 Tz. 4.2);
(c) Im Einklang mit der ISO/IEC 17065:2012 muss die Zertifizierungsstelle darüber hinaus eine dritte Seite im Sinne der ISO/IEC 17000:2004 sein. Eine dritte Seite ist eine Stelle, die ein unabhängiger Dritter ist, die den Zertifizierungsgegenstand prüft und von Interessen als Anwender dieses Gegenstands unabhängig ist. Gemäß Artikel R 17 Abs. 3 S. 1 des Beschlusses Nr. 768/2008/EG muss es sich bei einer Zertifizierungsstelle um einen unabhängigen Dritten handeln, der mit der Einrichtung, die er bewertet, in keinerlei Verbindung steht. Nach Absatz 4 des Artikels R 17 des Beschlusses Nr. 768/2008/EG dürfen eine Zertifizierungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter nicht Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der zu bewertenden Produkte oder Bevollmächtigter einer dieser Parteien sein, sofern diese Verbindung aufgrund geringer Erheblichkeit die Unparteilichkeit nicht in Frage stellt. Deswegen sind die notwendige Unparteilichkeit und Trennung der beteiligten Stellen sicherzustellen und zu dokumentieren. Keine dritte Seite ist eine Stelle, die Verträge mit den Zertifizierungskunden schließt. Somit können insbesondere Vergabestellen und Auftraggeber sowie deren Organisationen, die Vertragspartner sind oder sein können, nicht selbst Zertifizierungsstelle sein. Bei der Herbeiführung einer rechtlichen Trennung der Zertifizierungsstelle von einer solchen Organisation, gilt der folgende Absatz (4).

(4) Gemäß Tz. 4.2.7 der ISO/IEC 17065:2012 muss die Zertifizierungsstelle sicherstellen, dass Tätigkeiten rechtlich getrennter juristischer Personen, mit denen die Zertifizierungsstelle oder die juristische Person, der sie angehört, Beziehungen hat, die Unparteilichkeit ihrer Zertifizierungstätigkeiten nicht beeinträchtigen (s. DSK Tz. 4.2.7). Eine Zertifizierungsstelle, die einer juristischen Person (z. B. Verband oder eine Körperschaft des öffentlichen Rechts) angehört oder von einer juristischen Person kontrolliert wird oder sonstige Beziehungen zu einer juris-

tischen Person hat, deren Mitglieder oder Anteilseigner Hersteller, Anbieter, Auftragsverarbeiter oder Verantwortliche sind, die von dieser Zertifizierungsstelle zertifiziert werden, kann nur dann als unabhängige dritte Stelle gelten, wenn ihre Unabhängigkeit entsprechend Art. 43 Abs. 2 lit. a DSGVO bzw. Unparteilichkeiten entsprechend Tz. 3.13 der ISO/IEC 17065:2012 sowie die Abwesenheit jedweder Interessenkonflikte nachgewiesen ist. Dies kann der Fall sein, wenn

(a) die Zertifizierungsstelle rechtlich von der juristischen Person getrennt ist und
(b) das Personal der Zertifizierungsstelle und der juristischen Person getrennt sind und in keiner Weise für die Zertifizierungsstelle, insbesondere in Zertifizierungs-, Prüf- und Inspektionsverfahren, tätig wird (s. ISO/IEC 17065:2012 Tz. 4.2.8) und
(c) die oberste Leitung der Zertifizierungsstelle sich im Gesellschaftervertrag oder in der Satzung der Zertifizierungsstelle im Sinne des Tz. 4.2.5 der ISO/IEC 17065:2012 zur Unparteilichkeit verpflichtet und
(d) wenn die Satzung oder der Gesellschaftervertrag einen Passus zur Weisungsunabhängigkeit des Geschäftsführers und/oder des Leiters der Zertifizierungsstelle enthält und
(e) in Konkretisierung des Tz. 4.2.2 der ISO/IEC 17065:2012 kein wirtschaftliches Abhängigkeitsverhältnis zu den Mitgliedern der juristischen Person oder der juristischen Person selbst besteht.

§ 4.1.5 Wahrung der Vertraulichkeit

(1) Im Allgemeinen müssen die Zertifizierungstätigkeiten vertraulich durchgeführt werden. Daher müssen die Zertifizierungsstelle und ihre (ausgegliederten) Evaluatoren alle Anforderungen der ISO/IEC 17065:2012 Tz. 4.5 erfüllen und fortlaufend einhalten.

§ 4.1.6 Durchführung der Zertifizierungstätigkeiten unter nicht-diskriminierenden Bedingungen

(1) Zur Sicherstellung, dass grundsätzliche Regelungen und Verfahren, im Rahmen derer die Zertifizierungsstelle tätig ist, sowie ihre Verwaltung nicht-diskriminierend ist, müssen die Zertifizierungsstelle und ihre (ausgegliederten) Evaluatoren alle Anforderungen der ISO/IEC 17065:2012 Tz. 4.4 erfüllen und fortlaufend einhalten.

§ 4.1.7 Rechtliche Verantwortung

(1) Die Zertifizierungsstelle muss eine juristische Person oder ein festgelegter Teil einer juristischen Person sein, so dass die juristische Person für alle ihre Zertifizierungstätigkeiten rechtlich verantwortlich gemacht werden kann (s. ISO/IEC 17065:2012 Tz. 4.1.1).
(2) Eine Zertifizierungsstelle sollte in der Lage sein, der DAkkS oder der zuständigen Datenschutzaufsichtsbehörde nachzuweisen, dass sie über aktuelle Verfahren verfügt, die die Einhaltung der in den Akkreditierungsbedingungen festgelegten rechtlichen Verantwortlichkeiten, einschließlich der zusätzlichen Anforderungen in Bezug auf die Anwendung der DSGVO, nachweisen (EDPB Annex 1 Tz. 4.1.1).
(3) Die Zertifizierungsstelle ist ebenfalls Verantwortlicher oder Auftragsverarbeiter von personenbezogenen Daten (bspw. Daten vom Cloud-Anbieter) und muss daher in der Lage sein, den Nachweis für die Einhaltung der Verfahren und Maßnahmen gemäß der DSGVO zu erbringen, die speziell für die Kontrolle und Handhabung der personenbezogenen Daten der Cloud-Anbieter als Teil des Zertifizierungsprozesses gelten (EDPB Annex 1 Tz. 4.1.1).

§ 4.1.8 Haftung und Finanzierung

(1) Die Zertifizierungsstelle muss darlegen können, dass sie die Risiken, die aus ihren Zertifizierungstätigkeiten entstehen, beurteilt hat, und über angemessene Vorkehrungen (z. B. Versicherungen oder Rücklagen) verfügt, um in den geographischen Regionen, in denen sie tätig ist, die Verbindlichkeiten abzudecken, die aus ihren Tätigkeitsfeldern entstehen (s. ISO/IEC 17065:2012 Tz. 4.3.1, DSK Tz. 4.3, EDPB Annex 1 Tz. 4.3).
(2) Die Zertifizierungsstelle muss über die finanzielle Stabilität sowie Ressourcen verfügen, die für ihre Tätigkeiten erforderlich sind (s. ISO/IEC 17065:2012 Tz. 4.3.2).
(3) Die Zertifizierungsstelle hat ihre finanzielle Stabilität nachzuweisen (s. DSK Tz. 4.3, EDPB Annex 1 Tz. 4.2). Die Entscheidung hinsichtlich Auswahl und Benennung dieser Nachweisunterlagen liegt im Ermessen der DAkkS und der zuständigen Datenschutzaufsichtsbehörde. Die Nachweise müssen jährlich vorgelegt werden (s. EDPB Annex 1 Tz. 4.3).

(4) Die Zertifizierungsstelle muss über eine für den Umfang ihrer Tätigkeit angemessene Vermögensschadenshaftpflichtversicherung verfügen (s. DSK Tz. 4.3, EDPB Annex 1 Tz. 4.3). Die Berechnung der notwendigen Deckung hat auf einer Risikobetrachtung der Zertifizierungsstelle zu basieren.

§ 4.1.9 Bereitstellung von Informationen für die Öffentlichkeit

(1) Die Zertifizierungsstelle muss einen Geschäftsverteilungsplans der Zertifizierungsstelle vorhalten (s. DSK Tz. 8.11.1),

(i) um Auskunfts- oder Informationsersuchen oder
(ii) einen Kontakt bei einer Beschwerde zu einer erteilten Zertifizierung zu ermöglichen.

(2) Die Zertifizierungsstelle muss (durch Publikationen, elektronische Medien oder andere Mittel) auf Anfrage folgende Informationen aufrechterhalten und bereitstellen (s. ISO/IEC 17065:2012 Tz. 4.6):

(a) Informationen über (oder Verweis auf) dieses Konformitätsbewertungsprogramm, einschließlich Auswahl- und Ermittlungsverfahren; Regeln und Verfahren zur Erteilung, Aufrechterhaltung der Zertifizierung, Erweiterung oder Einschränkung der Zertifizierung; Aussetzung, Widerruf oder Verweigerung der Zertifizierung;
(b) eine Beschreibung der Mittel, durch die die Zertifizierungsstelle finanzielle Unterstützung erhält sowie allgemeine Informationen über die Gebühren, die gegenüber den Cloud-Anbietern erhoben werden;
(c) eine Beschreibung der Rechte und Pflichten der Cloud-Anbieter, einschließlich Anforderungen, Einschränkungen oder Beschränkungen zur Nutzung des Namens und des Konformitätszeichen sowie der Art und Weise, wie auf die Zertifizierung Bezug genommen wird;
(d) Informationen zu Verfahren zum Umgang mit Beschwerden und Einsprüchen im Einklang mit Art. 43 Abs. 2 lit. d DSGVO (s. DSK Tz. 4.6, EDPB Annex 1 Tz. 4.6). Dabei bezieht sich diese Veröffentlichungspflicht nicht nur auf einzelne Vorkommnisse, sondern auch auf die Struktur und Verfahrensweise zur Bearbeitung der Beschwerden durch die Zertifizierungsstelle.

4.2 Anforderungen an die Struktur und Ressourcen der Zertifizierungsstelle

§ 4.2.1 Anforderungen an die Organisationsstruktur, oberste Leitung und operative Lenkung

(1) Die Zertifizierungsstelle muss die Anforderungen gemäß ISO/IEC 17065:2012 Tz. 5.1 erfüllen und fortlaufend einhalten.

§ 4.2.2 Anforderungen an das Personalmanagement der Zertifizierungsstelle

(1) Die Zertifizierungsstelle muss eine ausreichende Anzahl an Personal beschäftigen oder Zugang dazu haben, um den personellen Bedarf ihrer Zertifizierungstätigkeiten abzudecken sowie zur Erfüllung der Zertifizierungsanforderungen.
(2) Die Zertifizierungsstelle muss die Anforderungen gemäß ISO/IEC 17065:2012 Tz. 6.1 erfüllen und fortlaufend einhalten.

§ 4.2.3 Anforderungen an personelle Kompetenzen

(1) Das Personal muss kompetent sein für die Aufgaben, die es ausführt, einschließlich der Durchführung der erforderlichen fachlichen Beurteilung sowie der Festlegung und Umsetzung von grundsätzlichen Regelungen (s. ISO/IEC 17065:2012 Tz.6.1.1.1).
(2) Die Anforderungen an die personellen Kompetenzen werden durch die ergänzenden Anforderungen der DSK in ihrer maßgeblichen Fassung festgelegt und müssen von der Zertifizierungsstelle fortlaufend eingehalten werden.
(3) Die Zertifizierungsstelle muss ein Verfahren für das Management der Kompetenzen des Personals, das in den Zertifizierungsprozess eingebunden ist, festlegen, einführen und aufrechterhalten (s. EDPB Annex 1 Tz. 9.2, DSK Tz. 8.10). Die Zertifizierungsstelle muss hierzu die Anforderungen der ISO/IEC 17065:2012 Tz. 6.1.2 erfüllen und fortlaufend einhalten. Dazu zählt insbesondere auch, dass die Kenntnisse des Personals für Evaluierung und Entscheidung auf aktuellem Stand gehalten werden müssen (s. DSK Tz. 6.1.2.1). Die fortlaufende Schulung des Personals, bspw. hinsichtlich der unter § 4.5.2 aufgeführten Entwicklungen,

nimmt somit eine besondere Stellung zur Aufrechterhaltung der Kompetenz ein und ist daher durchzuführen (s. DSK Tz. 8.10).

§ 4.2.4 Vertrag mit dem Personal

(1) Die Zertifizierungsstelle muss die Anforderungen gemäß ISO/IEC 17065:2012 Tz. 6.1.3 erfüllen und fortlaufend einhalten.

§ 4.2.5 Einbindung von externen Ressourcen (Outsourcing)

(1) Eine Zertifizierungsstelle kann eine ausgegliederte, unabhängige und fachlich kompetenten Prüfstelle oder (einzelne) externe Evaluatoren zur Durchführung der Auswahl- und/oder Ermittlungstätigkeiten gemäß ISO/IEC 17065:2012 Tz. 6.2.2 benennen.

(2) Die Prüfstelle und ausgegliederte Evaluatoren haben ein Vertragsverhältnis mit der Zertifizierungsstelle. Zwischen ihnen und einem zu zertifizierenden Cloud-Anbieter darf kein Vertragsverhältnis bestehen.

(3) Die Zertifizierungsstelle soll Auswahl- und Ermittlungstätigkeiten nur an Prüfstellen und Evaluatoren ausgliedern, welche die in diesem Konformitätsbewertungsprogramm beschriebenen Zertifizierungsanforderungen einhalten. Insbesondere sind die datenschutzspezifischen Anforderungen durch die Prüfstellen und Evaluatoren zu beachten (s. DSK Tz. 6.1.2.1, 6.2.2).

(4) Wenn die Zertifizierungsstelle Ermittlungstätigkeiten ausgliedert, müssen die Prüfstellen und ausgegliederte Evaluatoren insbesondere nach der entsprechenden internationalen Norm, insb. die ISO/IEC 17020 für die Inspektion, die ISO/IEC 17021 für die Durchführung von Audits und Managementsystemen, die ISO/IEC 17025 für die Prüfung, die ISO/IEC 17065 für Zertifizierungen, für den jeweiligen Geltungsbereich akkreditiert sein (s. ISO/IEC 17065:2012 Tz. 6.2, 7.4.5).

(5) Die Zertifizierungsanforderungen an die Unparteilichkeit des Personals, das die Auswahl- und Ermittlungstätigkeiten durchführt, die in diesem Programm festgelegt sind, müssen stets anwendbar sein.

(6) Die Zertifizierungsstelle muss:

(a) die Verantwortung für alle Tätigkeiten übernehmen, die an Prüfstellen und Evaluatoren ausgegliedert werden;
(b) die Durchführung von Auswahl- und Ermittlungstätigkeiten planen, steuern und überwachen;
(c) über dokumentierte Regelungen, Verfahren und Aufzeichnungen zur Qualifikation, Bewertung und Überwachung aller Prüfstellen und Evaluatoren verfügen, die ausgegliederte Dienstleistungen, die für Zertifizierungstätigkeiten genutzt werden, bereitstellen;
(d) eine Liste zugelassener Prüfstellen und Evaluatoren ausgegliederter Dienstleistungen führen;
(e) Korrekturmaßnahmen einführen für jegliche Verletzungen der Zertifizierungsvereinbarung und anderer Anforderungen dieses Programms durch Prüfstellen und Evaluatoren, von denen sie Kenntnis erlangt;
(f) den Cloud-Anbieter im Voraus über ausgegliederte Tätigkeiten informieren, um ihm eine Einspruchsmöglichkeit zu geben.

(7) Wenn die Qualifikation, Bewertung und Überwachung derjenigen Prüfstellen und Evaluatoren, die ausgegliederte Dienstleistungen bereitstellen, durch andere Organisationen durchgeführt werden (z. B. DAkkS oder zuständige Datenschutz-Aufsichtsbehörde), dann kann die Zertifizierungsstelle diese Qualifikation und Überwachung berücksichtigen, vorausgesetzt, dass:

(a) der Geltungsbereich für die vorgenommenen Arbeiten zutrifft;
(b) die Gültigkeit der Festlegungen zur Qualifikation, Bewertung und Überwachung in regelmäßigen Abständen, die von der Zertifizierungsstelle festgelegt werden, überprüft wird.

(8) Die Zertifizierungsstelle muss von Prüfstellen und ausgegliederten Evaluatoren, die Auswahl- oder Ermittlungstätigkeiten durchführen, fordern, einen Vertrag oder ein anderes Dokument zu unterzeichnen, durch das sich diese verpflichten (s. ISO/IEC 17065:2012 Tz. 6.1.3):

(a) die von der Zertifizierungsstelle festgelegten grundsätzlichen Regelungen und eingeführten Prozesse einzuhalten, einschließlich solcher, die sich auf die Vertraulichkeit und Unabhängigkeit von kommerziellen und sonstigen Interessen beziehen;

(b) ihre Tätigkeit nichtdiskriminierend, vertraulich und unparteilich auszuführen;
(c) jegliche frühere und/oder gegenwärtige Verbindungen ihrerseits oder seitens des Arbeitgebers mit:
    (i) einem Lieferanten oder Entwickler von Produkten, oder
    (ii) einem Anbieter oder Entwickler von Dienstleistungen, oder
    (iii) einem Betreiber oder Entwickler von Prozessen

    in Bezug auf die Auswahl- oder Ermittlungstätigkeiten eines Cloud-Anbieters, der sie zuzuordnen sind, anzugeben; und
(d) jede ihnen bekannte Situation offen zu legen, die es selbst oder die Zertifizierungsstelle vor Interessenkonflikte stellen könnte.

(9) Die Zertifizierungsstellen müssen diese Informationen als Eingaben berücksichtigen, um Gefährdungen bezüglich der Unparteilichkeit zu identifizieren, die durch die Tätigkeiten des jeweiligen Personals oder der Organisationen, die dieses Personal beschäftigt haben, entstehen.
(10) Die Zertifizierungsstelle kann bei Bedarf ein Verfahren der Zulassung von Prüfstellen und ausgegliederten Evaluatoren festlegen. In diesem Fall muss die Zulassung nach transparenten, nichtdiskriminierenden, objektiven Maßstäben erfolgen. Soweit die Zertifizierungsstelle ein Zulassungsverfahren durchführt, kann sie festlegen, dass sie Zertifizierungsaufträge nur annimmt, wenn die Auswahl- und/oder Ermittlungstätigkeiten durch von ihr zugelassenen Prüfstellen und Evaluatoren durchgeführt werden.

§ 4.2.6 Anforderungen an interne Ressourcen

(1) Die Zertifizierungsstelle muss die Anforderungen gemäß ISO/IEC 17065:2012 Tz. 6.2.1 erfüllen und fortlaufend einhalten.
(2) Wenn die Zertifizierungsstelle die Ermittlung mit ihren internen Ressourcen oder mit anderen Ressourcen, die unter ihrer direkten Kontrolle stehen, durchführt, muss sie insbesondere nach der entsprechenden internationalen Norm, insbes. die ISO/IEC 17025 für die Prüfung, die ISO/IEC 17021 für die Durchführung von Audits und Managementsystemen und die ISO/IEC 17020 für die Inspektion, für den jeweiligen Geltungsbereich akkreditiert sein (s. ISO/IEC 17065:2012 Tz. 6.2, 7.4.5).
(3) Falls für die Ermittlung (ggf. extern bereitgestellte) technische Einrichtungen (bspw. Server) und Anwendungen (bspw. Software zur Durchführung von technischen Tests) genutzt werden, muss die Zertifizierungsstelle sicherstellen, dass die zur Bereitstellung eines validen Ergebnisses erforderliche Messgenauigkeit und/oder Messunsicherheit erreicht werden. Die Eignung ist fortlaufend zu überprüfen. Die genutzten technischen Ressourcen müssen fortlaufend gewartet und ihre Funktionsfähigkeit sichergestellt werden.
(4) Bei der Verwendung von Informationssystemen zur Durchführung von Zertifizierungstätigkeiten muss sichergestellt sein, dass Verfahren zum Schutz der Integrität und Sicherheit der Daten eingeführt und umgesetzt sind.

4.3 Anforderungen an Zertifizierungstätigkeiten

§ 4.3.1 Management von Aufzeichnungen

(1) Die Zertifizierungsstelle muss Aufzeichnungen aufbewahren, um nachzuweisen, dass alle Zertifizierungsanforderungen an den Zertifizierungsprozess wirksam erfüllt worden sind (s. ISO/IEC 17065:2012 Tz. 7.12.1).
(2) Außerdem muss die Zertifizierungsstelle eine Statistik über abgeschlossene und abgebrochene Verfahren führen (s. DSK Tz. 7.12).
(3) Sämtliche Dokumentation der Zertifizierungsstelle muss vollständig, nachvollziehbar, aktuell und revisionssicher aufbewahrt werden (s. DSK Tz. 7.12). Dies gilt sowohl für abgeschlossene und ohne positive Entscheidung beendete, als auch für laufende Zertifizierungsverfahren. Für laufende Zertifizierungsverfahren muss zu erkennen sein, welche Zertifizierungskriterien erfüllt sind und welche noch nicht.
(4) Die Zertifizierungsstelle muss Aufzeichnungen vertraulich behandeln. Die Aufzeichnungen müssen in einer Weise transportiert, übersendet oder übertragen werden, die die Aufrechterhaltung der Vertraulichkeit sicherstellt (s. ISO/IEC 17065:2012 Tz. 7.12.2).
(5) Aufzeichnungen müssen mindestens für den laufenden und den vorangegangenen Zyklus aufbewahrt werden (s. ISO/IEC 17065:2012 Tz. 7.12.3). Bei einer Zertifizierungsgültigkeitsdauer von 3 Jahren (s. § 5.5.5) beträgt die Aufbewahrungsdauer also mindestens 3 Jahre zu Beginn eines neuen Zyklus und maximal 6 Jahre bei Beendigung des aktuellen Zyklus. Diese

Frist kann sich im Falle von Auseinandersetzungen zwischen der Zertifizierungsstelle und dem Cloud-Anbieter oder dem Cloud-Anbieter und der zuständigen Datenschutz-Aufsichtsbehörde über die Gültigkeit der Zertifizierung hinaus bis zum Abschluss dieses Verfahrens verlängern (s. DSK Tz. 7.12).

§ 4.3.2 Umgang mit Beschwerden und Einsprüchen im Rahmen des Zertifizierungsverfahrens

(1) Die Zertifizierungsstelle muss über ein dokumentiertes Verfahren verfügen, um Beschwerden und Einsprüche entgegenzunehmen, zu evaluieren sowie Entscheidungen über diese zu treffen (s. ISO/IEC 17065:2012 Tz. 7.13.1, EDPB Annex 1 Tz. 7.13, 9.3.3, DSK Tz. 8.11.2).

(2) Eine Beschwerde bezeichnet einen Ausdruck der Unzufriedenheit, der eine Antwort erwartet – jedoch in anderem Sinne als Einspruch – durch jede Person oder jede Organisation gegenüber einer Zertifizierungsstelle bezüglich der Tätigkeiten dieser Stelle (s. ISO/IEC 17000:2004 Tz. 6.5).

(3) Ein Einspruch stellt ein Verlangen des Cloud-Anbieters gegenüber einer Zertifizierungsstelle dar, ihre Entscheidung bezüglich des Zertifizierungsgegenstandes zu überprüfen (s. ISO/IEC 17000:2004 Tz. 6.4).

(4) Das Beschwerdemanagementsystem ist als integraler Bestandteil im Managementsystem zu etablieren (s. DSK Tz. 8.11.3); dieses muss insbesondere die Anforderungen aus ISO/IEC 17065:2013 Tz. 4.1.2.2 lit. c, 4.1.2.2 lit. j, 4.6 lit. d und 7.13 erfüllen und fortlaufend einhalten. Konsequenzen sind, dass

   (a) bei größeren Änderungen eine neue Risikobewertung erfolgt.
   (b) Eine solche Risikobewertung kann direkten Einfluss auf die eingesetzten Zertifizierungsgegenstände haben.

(5) Eine Beschreibung über die Struktur und Verfahrensweise zur Bearbeitung der Beschwerden und Einsprüche durch die Zertifizierungsstelle muss allen interessierten Parteien öffentlich zur Verfügung stehen (s. ISO/IEC 17065:2013 Tz. 4.6, 7.13, DSK Tz. 4.6).

(6) Das Verfahren zum Umgang mit Beschwerden und Einsprüchen muss mindestens die folgenden Maßnahmen enthalten, und die Zertifizierungsstelle muss sicherstellen, dass entsprechende Maßnahmen ergriffen werden (s. ISO/IEC 17065:2013 Tz. 7.13):

   (a) Verfahren zur Entgegennahme, zur Validierung, zur Untersuchung der Beschwerde oder des Einspruchs sowie zur Entscheidung, welche Maßnahmen als Antwort ergriffen werden müssen;
   (b) Maßnahmen zur Integration des Beschwerdemanagements des jeweiligen Cloud-Anbieters (s. DSK Tz. 4.1.2.2);
   (c) Aktivitäten zum Aufzeichnen der Beschwerden oder des Einspruchs, einschließlich der Maßnahmen, die zu ihrer Lösung ergriffen werden.

(7) Die Zertifizierungsstelle sollte ein leicht auffindbares und bedienbares Kontaktformular oder gleichwertige Alternativen auf ihrer Webseite zur Abgabe von Beschwerden einrichten.

(8) Bei Erhalt einer Beschwerde oder eines Einspruchs muss die Zertifizierungsstelle bestätigen, ob sich die Beschwerde oder der Einspruch auf Zertifizierungstätigkeiten bezieht, für die die Zertifizierungsstelle verantwortlich ist, und falls dem so ist, muss diese sich damit befassen und alle erforderlichen Folgemaßnahmen ergreifen, um die Beschwerde oder den Einspruch beizulegen (s. ISO/IEC 17065:2012 Tz. 7.13.2, 7.13.3, 7.13.9).

(9) Die Zertifizierungsstelle muss für das Erfassen und Verifizieren aller erforderlichen Informationen (soweit möglich) verantwortlich sein, um eine Entscheidung über die Beschwerde oder den Einspruch herbeizuführen (s. ISO/IEC 17065:2012 Tz. 7.13.4).

(10) Die Zertifizierungsstelle muss geeignete Fristen für die Beteiligten und für die durchzuführenden Maßnahmen definieren, entsprechend des Umfangs, der Reichweite und der Kritikalität der Beschwerde bzw. des Einspruchs, um den Prozess der Bearbeitung von Beschwerden und Einsprüchen zeitlich zu kontrollieren (s. DSK Tz. 7.13).

(11) Die Entscheidung, die die Beschwerde oder den Einspruch klärt, muss durch eine Person (oder mehrere Personen) erfolgen oder bewertet und genehmigt werden, die nicht in die Zertifizierungstätigkeiten, die sich auf die Beschwerde oder den Einspruch beziehen, einbezogen ist/sind (s. ISO/IEC 17065:2012 Tz. 7.13.5, DSK Tz. 7.13).

(12) Um sicherzustellen, dass es keinen Interessenkonflikt gibt, darf das Personal einschließlich derjenigen Personen, die in leitender Position tätig sind und die für einen Cloud-Anbieter Beratungen geleistet haben oder durch einen Cloud-Anbieter angestellt sind, nicht durch die

Zertifizierungsstelle eingesetzt werden, um die Lösung einer Beschwerde oder eines Einspruchs des betreffenden Cloud-Anbieters zu bewerten oder zu genehmigen, wenn sie innerhalb der letzten zwei Jahre in Beratungen oder in ein Arbeitsverhältnis gegenüber dem Cloud-Anbieter eingebunden waren (s. ISO/IEC 17065:2012 Tz. 7.13.6, DSK Tz. 7.13).

(13) Die Zertifizierungsstelle muss darlegen, wie die personelle Trennung zwischen Zertifizierungstätigkeit und der Bearbeitung von Einsprüchen und Beschwerden sichergestellt wird (s. DSK Tz. 7.13).

(14) Auf Anfrage durch den Beschwerde- oder Einspruchsführer oder einen weiteren Beteiligten muss die Zertifizierungsstelle Auskunft über den aktuellen Stand der Bearbeitung einer Beschwerde oder eines Einspruchs geben (s. DSK Tz. 7.13).

(15) Die Zertifizierungsstelle muss den Beschwerde- oder Einspruchsführer und alle weiteren Beteiligten formell über das Ergebnis und die Beendigung des Beschwerde- oder Einspruchsverfahrens informieren (s. ISO/IEC 17065:2012 Tz. 7.13.7, 7.13.8, DSK Tz. 7.13).

(16) Im Fall begründeter Beschwerden ist die zuständige Datenschutzaufsichtsbehörde zu informieren (s. DSK Tz. 8.11.3).

(17) Die Zertifizierungsstelle muss Beschwerden und Einsprüche sowie die Maßnahmen, die zu ihrer Lösung ergriffen werden, aufzeichnen und aufbewahren. Die Aufbewahrungsdauert sollte mindestens einem Zertifizierungszyklus entsprechen. Einzelne Vorkommnisse müssen in einer geeigneten Weise veröffentlicht werden (s. DSK Tz. 4.6).

(18) Der Programmeigner kann zur Klärung von Beschwerden und Einsprüchen herangezogen werden, wenn bspw. Unklarheit in Bezug auf Zertifizierungsanforderungen oder Zertifizierungskriterien herrscht. Der Programmeigner prüft, ob er zu Klärung entsprechende Informationen oder Ressourcen beitragen kann. Eine Pflicht zur Unterstützung durch den Programmeigner besteht nicht.

§ 4.3.3 Management von Veränderungen an Datenverarbeitungsvorgängen

(1) Die Zertifizierungsstelle verpflichtet den Cloud-Anbieter sie während der gesamten Gültigkeitsdauer der Zertifizierung unverzüglich über Veränderungen zu informieren, die seine Fähigkeit, die Zertifizierungskriterien zu erfüllen, beeinträchtigen könnte. Die Zertifizierungsstelle etabliert einen Prozess zur Entgegennahme und Behandlung von entsprechenden Meldungen durch einen Cloud-Anbieter. Beispiele für Veränderungen sind (s. ISO/IEC 17065:2012 Tz. 4.1.2.2):

(a) Veränderung bei dem rechtlichen, wirtschaftlichen oder organisatorischen Status oder die bei der Eigentümerschaft und Änderungen der tatsächlichen oder rechtlichen Verhältnisse (s. DSK Tz. 4.1.2.2);
(b) Veränderung bei Organisation und Management (z. B. Änderungen von Schlüsselpositionen, Entscheidungsprozessen oder technischem Personal);
(c) wesentliche Änderungen an Software oder Hardware, welche zur Erbringung der Datenverarbeitungsvorgänge erforderlich sind;
(d) wesentliche Änderungen hinsichtlich der Verarbeitung personenbezogener Daten;
(e) Änderungen der für den Zertifizierungsgegenstand einschlägigen Rechtsnormen sowie des Stands der Technik;
(f) Änderungen an Rechenzentren (bspw. Standortwechsel);
(g) Änderungen bei der Einbindung von Subauftragsverarbeitern mit Relevanz für den Datenverarbeitungsvorgang.

(2) Die Zertifizierungsstelle ist bei Hinweisen über solche Änderungen, die Einfluss auf die Konformitätsbewertungsaussage haben könnten verpflichtet, den Sachverhalt innerhalb von 4 Wochen zu ermitteln und geeignete Maßnahmen zu ergreifen (s. DSK Tz. 4.1.2.2). Die Zertifizierungsstelle hat darüber hinaus zu definieren, wie sichergestellt wird, dass in vergleichbaren Fällen vergleichbare Maßnahmen ergriffen werden. Geeignete Maßnahmen sind:

(a) Anwendung von Ermittlungsmethoden (s. § 5.2.4), um die Einhaltung der Zertifizierungskriterien, welche durch die Änderung betroffen sind, festzustellen (s. ISO/IEC 17065:2012 Tz.7.11.1); die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist. Die Anforderungen an eine Zwischenprüfung gemäß § 5.6.4 sind einzuhalten;
(b) die Zertifizierungsstelle kann dem Cloud-Anbieter eine Änderungszertifizierung empfehlen (s. § 5.6.9);

(c) bei Feststellung einer Nichtkonformität von Zertifizierungskriterien die Durchführung der unter § 5.6.4 beschriebenen Maßnahmen gemäß den dort festgelegten Anforderungen ergreifen.

§ 4.3.4 Management von Änderungen an rechtlichen Rahmenbedingungen

(1) Die Zertifizierungsstelle muss geeignete Maßnahmen ergreifen und fortlaufend durchführen, um Änderungen der rechtlichen Rahmenbedingungen, die ihn bzw. die Zertifizierung betreffen, zeitnah zu erkennen. Beispiele für Veränderungen sind (s. DSK Tz. 7.10, EDPB Annex 1 Tz. 7.10):

(a) Gesetzesnovellierungen;
(b) Erlass delegierter Rechtsakte der Europäischen Kommission;
(c) Entscheidungen des Europäischen Datenschutzausschusses;
(d) Gerichtsentscheidungen;
(e) Fortentwicklungen des Stands der Technik (soweit relevant für die künftige Zertifizierung und Überwachung).

(2) Die Zertifizierungsstelle muss dem Cloud-Anbieter Änderungen der rechtlichen Rahmenbedingungen, die ihn bzw. die Zertifizierung betreffen, zeitnah mitteilen (s. DSK Tz. 7.10).

(3) Die Zertifizierungsstelle ist bei Hinweisen über solche Änderungen, die Einfluss auf die Konformitätsbewertungsaussage haben könnten verpflichtet, den Sachverhalt zu ermitteln und geeignete Maßnahmen zu ergreifen (s. DSK Tz. 4.1.2.2). Geeignete Maßnahmen sind:

(a) Ermittlungsmethoden (s. § 5.2.4), um die Einhaltung der Zertifizierungskriterien, welche durch die Änderung betroffen sind, festzustellen (s. ISO/IEC 17065:2012 Tz.7.11.1); die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist. Die Anforderungen an eine Zwischenprüfung gemäß § 5.6.4 sind einzuhalten;
(b) die Zertifizierungsstelle kann dem Cloud-Anbieter eine Änderungszertifizierung empfehlen (s. § 5.6.9);
(c) bei Feststellung einer Nichtkonformität von Zertifizierungskriterien kann sie die unter § 5.6.4 beschriebenen Maßnahmen gemäß den festgelegten Anforderungen ergreifen.

(4) Die Zertifizierungsstelle hat darüber hinaus zu definieren, wie sie sicherstellt, dass in vergleichbaren Zertifizierungsverfahren (auch im Fall einer Änderung der Zertifizierungsanforderungen) vergleichbare Prüfungen durchgeführt werden (s. DSK Tz. 7.10).

(5) Die Zertifizierungsstelle informiert zudem den Programmeigner falls die Änderungen einen Einfluss auf die Zertifizierungsanforderungen oder Zertifizierungskriterien haben, oder von großer Bedeutung sind. Stellt der Programmeigner Änderungen fest, informiert er die Zertifizierungsstellen entsprechend (s. § 2.1.4).

§ 4.3.5 Management von Änderungen an diesem Programm

(1) Der Programmeigner kann Änderungen an den festgelegten Zertifizierungskriterien, Zertifizierungsanforderungen und diesem Programm durchführen (bspw. aufgrund von Änderungen an den rechtlichen Rahmenbedingungen). Der Programmeigner informiert daraufhin die Zertifizierungsstelle.

(2) Wenn dieses Konformitätsbewertungsprogramm neue oder überarbeitete Zertifizierungsanforderungen einführt, verpflichtet sich die Zertifizierungsstelle zur raschen Umsetzung dieser Anforderungen. Betreffen diese Änderungen auch ausgegliederte Evaluatoren, so muss die Zertifizierungsstelle die ausgegliederten Evaluatoren über die Änderungen informieren und sicherstellen, dass in angemessener Zeit die Anforderungen umgesetzt und anschließend fortlaufend durch die ausgegliederten Evaluatoren eingehalten werden.

(3) Eine Zertifizierungsstelle muss geeignete Prozesse etablieren, um auf Änderungen dieses Programm zu reagieren. Hierzu zählen unter anderem folgende Maßnahmen:

(a) Eine Zertifizierungsstelle informiert einen Cloud-Anbieter über Änderungen an den Zertifizierungskriterien oder diesem Programm, insoweit diese Änderungen ihn oder seine Zertifizierung betreffen;
(b) Eine Zertifizierungsstelle leitet Maßnahmen ein, um Änderungen an den Zertifizierungsanforderungen zeitnah umzusetzen;
(c) Die Zertifizierungsstelle ist verpflichtet bei Änderungen an Zertifizierungskriterien, die Einfluss auf die Konformitätsbewertungsaussage haben könnten, den Sachverhalt für jeden

zertifizierten Datenverarbeitungsvorgang zu ermitteln und geeignete Maßnahmen zu ergreifen. Geeignete Maßnahmen sind:

(i) Ermittlungsmethoden (s. § 5.2.4), um die Einhaltung der Zertifizierungskriterien, welche durch die Änderung betroffen sind, festzustellen (s. ISO/IEC 17065:2012 Tz.7.11.1); die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist. Die Anforderungen an eine Zwischenprüfung gemäß § 5.6.4 sind einzuhalten;
(ii) die Zertifizierungsstelle kann dem Cloud-Anbieter eine Änderungszertifizierung empfehlen (s. § 5.6.9);
(iii) bei Feststellung einer Nichtkonformität von Zertifizierungskriterien, welche durch die Änderung betroffen sind, kann sie die unter § 5.6.4 beschriebenen Maßnahmen gemäß den dort festgelegten Anforderungen ergreifen.

§ 4.3.6 Management der Kommunikation mit der zuständigen Aufsichtsbehörde

(1) Die Zertifizierungsstelle muss Verfahren und Verantwortlichkeiten festlegen, um die zuständigen Aufsichtsbehörden bei notwendigen Zertifizierungstätigkeiten (bspw. Einspruch bei der Erteilung der Zertifizierung, s. § 5.5.6) einzubeziehen.
(2) Anfragen der Aufsichtsbehörden müssen zeitnah entgegengenommen, dokumentiert und beantwortet werden.

4.4 Anforderungen zur Nutzung dieses Programms

§ 4.4.1 Durchführung von Zertifizierungen nach diesem Programm

(1) Der Programmeigner stellt dieses Programm zu nicht-diskriminierenden Bedingungen interessierten Zertifizierungsstellen zur Verfügung, im Einklang mit den Vorgaben von Art. 101 und 106 AEUV (FRAND-Vereinbarung).
(2) Der Programmeigner schließt eine Nutzungsvereinbarung mit interessierten Zertifizierungsstellen (s. ISO/IEC 17030:2009 Tz. 4.3).
(3) Die Zertifizierungsstelle verpflichtet sich in dieser Nutzungsvereinbarung zur Einhaltung der Anforderungen dieses Programms (s. ISO/IEC 17030:2009 Tz. 7.2).

§ 4.4.2 Führen eines Verzeichnisses von zertifizierten Datenverarbeitungsvorgängen

(1) Die Zertifizierungsstelle führt ein öffentlich einsehbares Register mit zertifizierten Datenverarbeitungsvorgängen, um eine Rückverfolgung durch interessierte Parteien zu ermöglichen (s. ISO/IEC 17030:2009 Tz. 5.3, Tz. 7.1).
(2) Für jeden zertifizierten Datenverarbeitungsvorgang sollten folgende Informationen bei Erteilung der Zertifizierung hinterlegt sein, welches mindestens die folgenden Elemente enthalten (s. ISO/IEC 17065:2012 Tz. 7.8, DSK Tz. 7.8, ISO/IEC 17030:2009 Tz. 5):

(a) die eindeutige Bezeichnung des Zertifizierungsgegenstands;
(b) die eindeutige Bezeichnung des Cloud-Anbieters, inkl. Name und Anschrift des Cloud-Anbieters;
(c) die Zertifizierungsstelle, ggf. Logo der Zertifizierungsstelle;
(d) die maßgebliche Fassung des AUDITOR-Kriterienkatalogs, nach dem die Konformität zertifiziert wurde;
(e) die Bezeichnung der maßgeblichen Fassung des Konformitätsbewertungsprogramms;
(f) eine Zertifizierungsnummer;
(g) die Gültigkeitsdauer der Zertifizierung, inkl. Datum der Entscheidung und Ende der Zertifizierung;
(h) die Zertifizierungsaussage, wonach die zertifizierten Datenverarbeitungsvorgänge die einschlägigen Vorgaben der DSGVO und des BDSGs gemäß dem AUDITOR-Kriterienkatalog in der jeweiligen Fassung für eine konkrete Schutzklasse und eine konkrete Wiederherstellbarkeitsklasse erfüllt;
(i) Informationen über die Erst- bzw. Rezertifizierung (bspw. Datum der Erstzertifizierung, Anzahl der Rezertifizierungen);
(j) Informationen über die eventuelle Einbindung ausgegliederter Evaluatoren;
(k) Ansprechstellen für Beschwerden, bspw. im Falle einer Feststellung der Nichtkonformität;
(l) Kurzangabe zu Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung;

(m) ein Kurzgutachten bzgl. des jeweiligen Zertifizierungsergebnisses, aus dem sich der genaue Zertifizierungsgegenstand (inklusive Versions- oder Funktionsstand), das Evaluationsverfahren (inklusive der der Zertifizierung zugrundliegenden Kriterien (ggf. mit Versionsangabe) und einer Angabe über Kriterien, die nicht anwendbar waren) und das Evaluationsergebnis ableiten lassen (s. DSK Tz. 7.8).

(3) Auf Anfrage muss die Zertifizierungsstelle zeitnah interessierten Parteien Informationen zur Erläuterung der Bedeutung des Konformitätszeichens geben und mitteilen können, ob ein ausgestelltes Konformitätszeichen weiterhin gültig ist (s. ISO/IEC 17030:2009 Tz. 7.1). Auf Fragen oder Bedenken interessierter Parteien hinsichtlich des Konformitätszeichens muss zeitnah und gezielt geantwortet werden.

(4) Alle Informationen müssen in einem elektronischen Verzeichnis hinterlegt werden, welches über das Internet erreichbar und öffentlich einsehbar ist. Ein leichter Zugang zu diesem elektronischen Verzeichnis sollte ermöglicht werden (bspw. ohne vorherige Registrierung).

(5) Die Zertifizierungsstelle muss dem Programmeigner mitteilen, wie er das Verzeichnis aufrufen kann (bspw. Mitteilung der Internetadresse).

§ 4.4.3 Verwendung von AUDITOR-Konformitätszeichen

(1) Die Zertifizierungsstelle muss durch rechtlich durchsetzbare Vereinbarungen fordern, dass der Cloud-Anbieter die ausgestellten Konformitätszeichen auf Webseiten, (gedruckten) Publikationen, Dokumente und sonstigen Werbematerialien verwenden darf (s. ISO/IEC 17030:2009 Tz. 5.6), insofern keine Missverständnisse, Unklarheiten und Irreführungen erzeugt werden und alle Regelungen dieses Programms und etwaiger Anforderungen in der Nutzungsvereinbarung zwischen der Zertifizierungsstelle und dem Programmeigner eingehalten werden.

(2) Insbesondere wenn sich ein Konformitätszeichen nur auf bestimmte Datenverarbeitungsvorgänge eines Cloud-Dienstes bezieht oder andere Einschränkungen des Geltungsbereichs vorliegen (bspw. bestimmte Standorte), muss die Zertifizierungsstelle den Cloud-Anbieter verpflichten in seiner Kommunikation sicherzustellen, dass es zu keinen Missverständnissen kommt und sich das Zeichen nicht auf den gesamten Cloud-Dienst, allen Standorten oder anderen Geltungsbereiche bezieht (s. ISO/IEC 17030:2009 Tz. 5.5).

(3) Ein Anbringen von Konformitätszeichen auf dem Produkt oder der Produktverpackung ist nicht gestattet (s. ISO/IEC 17030:2009 Tz. 5.4).

(4) Die Zertifizierungsstelle muss mit geeigneten Maßnahmen sicherstellen, dass ausgestellte Konformitätszeichen den Anforderungen des Programms entsprechen (s. ISO/IEC 17065:2012 Tz. 4.1.3).

(5) Die Zertifizierungsstelle muss Maßnahmen ergreifen, um Missverständnisse, Unklarheiten und Irreführungen hinsichtlich der Konformitätszeichen, die zu einer Einschränkung dessen Wirksamkeit führen könnten, zu minimieren (s. ISO/IEC 17030:2009 Tz. 4.2).

(6) Die Zertifizierungsstelle etabliert Verfahren zur Überwachung der korrekten Verwendung des Konformitätszeichens für die Gültigkeitsdauer (s. ISO/IEC 17030:2009 Tz. 4.2, 7.2, 7.3). Hierzu zählen insbesondere:

(a) die stichprobenartige Untersuchung der korrekten Werbung mit den Konformitätszeichen bei der initialen Erteilung;

(b) die Bereitstellung einer Kontaktstelle (bspw. Kontaktformular, E-Mail-Adresse etc.) zur Meldung der unrechtmäßigen oder inkorrekten Verwendung von Konformitätszeichen durch interessierte Parteien;

(c) Maßnahmen zu ergreifen bei und Aufzeichnungen anfertigen von allen Beschwerden, die die Verwendung des Konformitätszeichens betreffen;

(d) die stichprobenartige Überprüfung der korrekten Verwendung im Rahmen der Überwachung;

(e) Maßnahmen zu ergreifen, um Missbräuche des Konformitätszeichens zu beheben, einschließlich Aufforderungen zu Korrektur und Korrekturmaßnahme, Aussetzung und Widerrufs der Zertifizierung, Veröffentlichung des Verstoßes oder angemessene rechtliche Maßnahmen. Dazu zählt auch der Missbrauch des Konformitätszeichens durch eine Partei, die keinen Vertrag mit der Zertifizierungsstelle hat;

(7) Inkorrekte Bezugnahme oder irreführende Verwendung von Konformitätszeichen, die in Veröffentlichungen oder anderen Publikationen gefunden wurden, müssen dem Programmeigner mitgeteilt werden.

§ 4.4.4 Berichterstattung an den Programmeigner

(1) Die Zertifizierungsstelle ist verpflichtet, dem Programmeigner mindestens jedes Jahr einen Kurzbericht über die Ausführung des Programms zur Programmverbesserung zu übersenden. In diesem Bericht müssen mindestens folgende Informationen enthalten sein:

(a) Anzahl an zertifizierten Datenverarbeitungsvorgängen;
(b) eine kurze Zusammenfassung über wesentliche Gründe für Beschwerden und Einsprüche;
(c) eine kurze Zusammenfassung der wesentlichen Gründe für die Feststellung der Nichtkonformität mit den Zertifizierungskriterien;
(d) sofern vorhanden offene Probleme oder Klärungsbedarf in Bezug auf dieses Programm;
(e) sofern vorhanden Vorschläge zur Verbesserung des Programms.

§ 4.4.5 Werbung mit und Verweis auf dieses Programm

(1) Zertifizierungsstellen und zertifizierte Cloud-Anbieter können auf dieses Programm verweisen, insofern keine Missverständnisse, Unklarheiten und Irreführungen erzeugt werden.
(2) Ein Verweis sollte auf die öffentlichen Einträge zu diesem Programm bei der DAkkS (bspw. Akkreditierungsprogramm der DAkkS) oder dem Webauftritt des Programmeigners erfolgen.
(3) Die maßgebliche Fassung des Konformitätsbewertungsprogramm und ein Datum für den Tag des Verweises sind anzugeben.
(4) Der Programmeigner ist bei einem Verweis zeitnah (innerhalb von 14 Tagen) informell zu informieren (bspw. per E-Mail).

4.5 Managementsystemanforderungen

§ 4.5.1 Etablierung eines Managementsystems

(1) Die Zertifizierungsstelle muss ein Managementsystem aufbauen und aufrechterhalten, welches die Fähigkeit besitzt, die Anforderungen nach ISO/IEC 17065:2012 Tz. 8.1 entweder in Übereinstimmung mit Option A oder Option B konsequent zu erfüllen und die Anwendung zu dokumentieren, evaluieren, kontrollieren und selbstverantwortlich zu überwachen (s. DSK Tz. 8.1, ‚Kapitel 8 ', EDBP Tz. 8). Unabhängig von der gewählten Option muss das Managementsystem die Anforderungen dieses Programms erfüllen. Dazu müssen Prozesse entsprechend der vorherigen Kapitel im eigenen Management der Zertifizierungsstelle umgesetzt werden. Dazu gehören insbesondere (s. DSK Tz. 8.1.1):

(a) Überwachung, Kontrolle, Evaluierung und Verbesserung der Struktur der internen Abläufe der Zertifizierungsstelle mit Fortschreibung der entsprechenden intern geführten Nachweise;
(b) Management des Erlöschens oder des Widerrufs der Akkreditierung und die sofortige Information der zertifizierten Cloud-Anbieter hierrüber (s. EDPB Annex 1 Tz. 9.3.4);
(c) Verwaltung des Beschwerdemanagements;
(d) Aussetzung und Widerruf der Zertifizierung und Dokumentation der Gründe;
(e) Vertragsmanagement;
(f) Sicherstellung der Unabhängigkeit (Unparteilichkeit/finanzielle Stabilität) und Management der entsprechenden Nachweise;
(g) Veröffentlichung von Zertifizierungsentscheidungen etc.;
(h) Ressourcen (Personalkompetenz und externe Ressourcen);
(i) Antragsmanagement;
(j) Überwachung von Änderungen mit Auswirkungen auf Zertifizierungen;
(k) Überwachung der Verwendung von ausgestellten Konformitätszeichen.

(2) Dazu muss das Managementsystem eine Methodik vorgeben, wie diese Vorgaben datenschutzkonform erreicht, kontrolliert, auch fortwährend bei der Zertifizierungsstelle selbst geprüft werden können (s. DSK ‚Kapitel 8').
(3) Diese Managementprinzipien und deren dokumentierte Umsetzung müssen im Akkreditierungsverfahren und danach jederzeit auf Wunsch der Datenschutzaufsichtsbehörde von der Zertifizierungsstelle u.a. während einer Untersuchung in Form von Datenschutzüberprüfungen (Art. 58 Abs. 1 lit. b DSGVO) oder einer Überprüfung der nach Art. 42 Abs. 7 DSGVO erteilten Zertifizierungen (Art. 58 Abs. 1 lit. c DSGVO) nachvollziehbar sein und offengelegt werden (Art. 58 DSGVO) (s. DSK ‚Kapitel 8').

§ 4.5.2 Fortschreibung der Evaluationsmethoden

(1) Die Zertifizierungsstelle muss Verfahren zur Lenkung der Fortschreibung der Evaluationsmethoden zur Anwendung im Rahmen der Evaluierung (s. ISO/IEC 17065:2013 Tz. 7.4) festlegen (s. DSK Tz. 8.9, EDPB Annex 1 Tz. 9.1). Die Fortschreibung hat im Zuge der Änderung der rechtlichen Rahmenbedingungen, der relevanten Risikoquellen, des Stands der Technik und der Implementierungskosten von TOM zu erfolgen.

(2) Die Verfahren müssen die erforderlichen Lenkungsmaßnahmen festlegen, um sicherzustellen, dass (s. DSK Tz. 8.9.2):

(a) alle relevanten Änderungen der rechtlichen Rahmenbedingungen (gemäß ISO/IEC 17065:2013 Tz. 7.4 und den dazugehörigen Erweiterungen in diesem Programm),
(b) Vertragsbestandteile zwischen Cloud-Anbieter und Zertifizierungsstelle,
(c) alle relevanten neu auftretenden (Kategorien von) Risikoquellen und Schwachstellen der Informationstechnik sowie
(d) der Fortschritt des Stands der Technik in Bezug auf Verarbeitungstätigkeiten und technische und organisatorische Maßnahmen, die zur Sicherstellung der Einhaltung der gesetzlichen Anforderungen, insbesondere im Hinblick auf die Umsetzung der Datenschutzgrundsätze und die Sicherheit der Verarbeitung angewandt werden können,

erfasst, dokumentiert und bewertet sowie in den Evaluationsmethoden abgebildet werden.

(3) Änderungen bzw. Änderungsprozesse und deren Gründe müssen dokumentiert werden, um diese nachvollziehen zu können (s. ISO/IEC 17065:2013 Tz. 7.10, DSK Tz. 8.11.2).

(4) Daneben ist sicherzustellen, dass im Rahmen des Managementsystems Änderungen von Anforderungen der Datenschutz-Aufsichtsbehörde und des Datenschutzausschusses an Kriterienkatalogen und Zertifizierungsverfahren überwacht werden und diese Änderungen umgehend in die eigenen Verfahren der Zertifizierungsstelle integriert werden (s. DSK Tz. 8.9.2). Eine Abstimmung mit dem Programmeigner ist in diesen Fällen erforderlich. Die Akkreditierungsstelle und die zuständige Datenschutzaufsichtsbehörde sind über Änderungen zu informieren.

(5) Auch muss durch die Zertifizierungsstelle sichergestellt werden, dass Rechtsakte und Vorgaben vom Datenschutzausschuss oder von Datenschutz-Aufsichtsbehörden zeitnah zur Kenntnis genommen werden und die umgehende Umsetzung veranlasst wird (s. DSK Tz. 8.9.2). Die Akkreditierungsstelle und die zuständigen Datenschutz-Aufsichtsbehörde müssen hierüber informiert werden.

(6) Dokumentationen zur Fortschreibung der Evaluationsmethoden müssen auf Anfrage der zuständigen Datenschutzaufsichtsbehörde offengelegt werden (s. DSK Tz. 8.11.2).

5 Anforderungen an den Zertifizierungsprozess

Der AUDITOR-Zertifizierungsprozess umfasst die sequentiellen Prozessstufen Auswahl (Nr. 5.1), Ermittlung (Nr. 5.2), Bewertung (Nr. 5.3), Entscheidung (Nr. 5.4) und Bestätigung (Nr. 5.5). Im Anschluss werden fortlaufende Überwachungstätigkeiten (Nr. 5.6) durchgeführt.

Nr. 5.1 Im Rahmen der **Auswahl** finden planende und vorbereitende Tätigkeiten durch (ausgegliederte) Evaluatoren statt, um für die nachfolgende Ermittlungsfunktion alle erforderlichen Informationen und Eingangsgrößen sammeln oder bereitstellen zu können, inklusive der Darstellung und Abgrenzung des Zertifizierungsgegenstands (s. ISO/IEC 17000:2004 Tz. A.2.1).

Nr. 5.2 Bei der **Ermittlung** werden eine oder mehrere Ermittlungsmethoden (z.B. Dokumentprüfung oder Audit) durch (ausgegliederte) Evaluatoren durchgeführt, um vollständige Informationen über die Erfüllung der im AUDITOR-Kriterienkatalog festgelegten Zertifizierungskriterien durch die Datenverarbeitungsvorgänge oder ihre Stichproben zu erhalten (s. ISO/IEC 17000:2004 Tz. A.3.1).

Nr. 5.3 Durch eine **Bewertung** verifizieren die Entscheider, ob die Auswahl- und Ermittlungstätigkeiten und deren Ergebnisse hinsichtlich der Erfüllung der festgelegten Zertifizierungskriterien durch die Datenverarbeitungsvorgänge geeignet, angemessen und wirksam sind (s. ISO/IEC 17000:2004 Tz. A.4).

Nr. 5.4 Die Entscheider fallen im Anschluss eine **Entscheidung** über die Erteilung der Zertifizierung, auf Grundlage der Ermittlung und der Bewertung (s. ISO/IEC 17000:2004 Tz. 5.2).

Nr. 5.5 Bei der **Bestätigung** erteilt die Zertifizierungsstelle die AUDTOR-Konformitätszeichen als Nachweis, dass die Erfüllung festgelegter Anforderungen nachgewiesen wurde (s. ISO/IEC 17067:2013 Tz. 5.1.1).

Nr. 5.6 Eine **Überwachung** umfasst systematische, sich wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Konformitätsaussage (s. ISO/IEC 17000:2004 Tz. 6.1).

5.1 Auswahl

§ 5.1.1 Bearbeitung und Bewertung des Zertifizierungsantrags

(1) Antragsberechtigt für eine Zertifizierung ist der Cloud-Anbieter als Auftragsverarbeiter (s. DSK Tz. 7.2).

(2) Die Zertifizierungsstelle muss einen Prozess zur Bewertung über die Annahme oder Ablehnung von Zertifizierungsanträgen etablieren. Hierbei sind auch die anwendbaren Gründe für eine Ablehnung zu spezifizieren, um eine mögliche Willkür bei der Bewertung zu unterbinden (s. ISO/IEC 17065:2012 Tz. 4.4.3), dazu zählen bspw.

(a) dass der Cloud-Anbieter an illegalen Aktivitäten beteiligt ist;
(b) der Cloud-Anbieter wiederholt gegen die AUDITOR-Zertifizierungskriterien verstoßen hat;
(c) oder ähnliche auf den Cloud-Anbieter bezogene Probleme nachweislich vorliegen.

(3) Die Zertifizierungsstelle muss es ablehnen, eine bestimmte Zertifizierung auszuführen, wenn

(a) ihr die Kompetenz oder Fähigkeit für die Zertifizierungstätigkeiten, die sie ausführen muss, fehlen (s. ISO/IEC 17065:2012 Tz. 7.3.4);
(b) die Mittel zur Durchführung aller Auswahl- und Ermittlungstätigkeiten fehlen; oder
(c) ihre Unparteilichkeit gefährdet ist.

(4) Die Annahme eines Zertifizierungsantrags darf weder von der Größe des Cloud-Anbieters oder von der Mitgliedschaft in einer Vereinigung oder Gruppe abhängig sein, noch darf die Zertifizierung von der Anzahl der bereits erteilten Zertifizierungen abhängen (s. ISO/IEC 17065:2012 Tz. 4.4.3). Es darf keine unlauteren finanziellen oder anderen Bedingungen geben.

(5) Die Zertifizierungsstelle bewertet nicht die Beantragung einer spezifischen Schutzklasse oder Widerherstellungsklasse. Diese Wahl obliegt alleinig dem Cloud-Anbieter.

(6) Die Zertifizierungsstelle muss Aufzeichnungen über die Begründung der Entscheidung, einen Zertifizierungsantrag anzunehmen oder abzulehnen, führen.

§ 5.1.2 Zertifizierungsvereinbarung

(1) Die Zertifizierungsstelle muss eine rechtlich durchsetzbare Zertifizierungsvereinbarung zur Bereitstellung von Zertifizierungstätigkeiten mit dem Cloud-Anbieter geschlossen haben (s. ISO/IEC 17065:2012 Tz. 4.1.2).

(2) Die Zertifizierungsstelle muss Prozesse zum Abschluss, zur Änderung und zur Überwachung der Zertifizierungsvereinbarungen etablieren und durchführen (s. DSK Tz. 7.2, 7.3).
(3) Die Zertifizierungsvereinbarung legt die maßgebliche Fassung des AUDITOR-Kriterienkatalogs fest.
(4) Die Zertifizierungsvereinbarung legt dieses Programm als maßgebliche Verfahrensregelung fest, insbesondere in Hinblick auf die Erteilung, Ablehnung, Aussetzung, Einschränkung, Überwachung und den Widerruf der Zertifizierung (s. EDPB Annex 1 Tz. 4.1.2).
(5) Die Zertifizierungsvereinbarung muss die Verantwortlichkeiten der Zertifizierungsstelle, ggf. der eingebundenen, ausgegliederten Evaluatoren und des Cloud-Anbieters berücksichtigen und eindeutig voneinander abgrenzen (s. ISO/IEC 17065:2012 Tz. 4.1.2).
(6) Die Zertifizierungsvereinbarung fordert die Mitteilungspflichten (s. § 5.1.3) des Cloud-Anbieters.
(7) Die Zertifizierungsvereinbarung enthält eine genaue Beschreibung des Zertifizierungsgegenstandes und die beantragte Schutzklasse und Wiederherstellbarkeitsklasse (s. § 5.1.4).
(8) Die Zertifizierungsvereinbarung listet die Zertifizierungskriterien auf, welche auf den spezifischen Zertifizierungsgegenstand nicht angewendet werden können, insofern diese bereits bekannt sind (s. hierzu § 5.1.5). Die Nichtanwendbarkeit ist zu begründen.
(9) Soweit der Cloud-Anbieter die Anerkennung von Zertifikaten für Bestandteile seiner Datenverarbeitungsvorgänge anstrebt (s. § 5.1.7), sind diese Zertifikate unter genauer Bezeichnung des anzuerkennenden Zertifikats und des Bestandteils seiner Datenverarbeitungsvorgänge, für die die Anerkennung gewünscht wird, in der Vereinbarung aufzunehmen.
(10) Die geplanten Ermittlungsmethoden unter Berücksichtigung des auf den Cloud-Anbieter anwendbaren Datenschutzrechts werden vertraglich in der Zertifizierungsvereinbarung festgehalten (s. DSK Tz. 7.4).
(11) Beauftragt die Zertifizierungsstelle ausgegliederte Evaluatoren zur Durchführung des Ermittlungsverfahrens gemäß ISO/IEC 17065:2012 Tz. 6.2.2 ist dies in der Vereinbarung zu dokumentieren.
(12) Die Zertifizierungsvereinbarung beschreibt die Folgen der Aussetzung oder Zurückziehung der Akkreditierung der Zertifizierungsstelle gemäß § 4.1.1. Die Zurückziehung einer Akkreditierung hat Konsequenzen für die Cloud-Anbieter als Kunden der Zertifizierungsstelle. Deshalb ist in der Zertifizierungsvereinbarung darauf hinzuweisen und verbindlich zu regeln, dass die Zertifizierung des Cloud-Anbieters abhängig von der Akkreditierung der Zertifizierungsstelle ist. Die Aussetzung oder Zurückziehung der Akkreditierung führt zur Ungültigkeit der Zertifizierung (s. DSK Tz. 4.1.2.2, EDPB Annex 1 Tz. 4.1.2).
(13) Die Zertifizierungsvereinbarung beschreibt das anzuwendende Konzept des Transfers von Zertifizierungen bei Erlöschen der Akkreditierung im Sinne der Art. 43 DSGVO (s. § 4.1.1), inklusive der Begutachtung des Transfers durch die DAkkS (s. DSK Tz. 4.1.2.2).
(14) Die Zertifizierungsvereinbarung regelt die Veröffentlichung von Informationen gemäß Art. 42 Abs. 8 und Art. 43 Abs. 5 DSGVO durch die Zertifizierungsstelle (s. EDPB Annex 1 Tz. 4.1.2).
(15) Die Zertifizierungsvereinbarung legt fest, dass ein Cloud-Anbieter einer zuständigen Datenschutz-Aufsichtsbehörde vollständige Einsicht in die Unterlagen des Zertifizierungsprozesses gewährt, dazu zählen auch vertrauliche Informationen über die Einhaltung der Anforderungen (s. EDPB Annex 1 Tz. 4.1.1). Der Cloud-Anbieter muss vorurteilsfrei die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde anerkennen (s. EDPB Annex 1 Tz. 4.1.1).
(16) Die Zertifizierungsstelle muss sicherstellen, dass ihre Zertifizierungsvereinbarung von dem Cloud-Anbieter fordert, mindestens Folgendes einzuhalten (s. ISO/IEC 17065:2012 Tz. 4.1.2):

   (a) die Zertifizierungskriterien fortlaufend zu erfüllen (s. DSK Tz. 4.1.2.2, EDPB Annex 1 Tz. 4.1.1); einschließlich der Umsetzung entsprechender Änderungen, wenn diese durch die Zertifizierungsstelle mitgeteilt werden (s. ISO/IEC 17065:2012 Tz. 4.1.2.2);
   (b) alle notwendigen Vorkehrungen zu treffen für
      (i) die Durchführung der Ermittlung und regelmäßigen Überwachung (gemäß der Regelungen zur Überwachung in Nr. 5.6), einschließlich der Berücksichtigung der Prüfung der Dokumentation und Aufzeichnungen, des Zugangs zu der entsprechenden Ausstattung, dem/den Standort(en), dem/den Bereich(en) und dem Personal, und den Subauftragsverarbeitern des Cloud-Anbieters (s. ISO/IEC 17065:2012 Tz. 4.1.2.2, DSK Tz. 4.1.2.2);
      (ii) (wo zutreffend) die Teilnahme von Beobachtern (z. B. Akkreditierungsbegutachter oder Auditoren in Ausbildung);
      (iii) die Untersuchung und Behandlung von Beschwerden (s. ISO/IEC 17065-1:2013 Tz. 7.13). Konkrete Ausführungen zur Struktur und dem Verfahren für

das Beschwerdemanagement des Cloud-Anbieters, insbesondere Verfahren zur Integration des Beschwerdemanagements mit der Zertifizierungsstelle (s. § 4.3.2), sind in der Zertifizierungsvereinbarung festzuhalten (s. DSK Tz. 4.1.2.2, EDPB Annex 1 Tz. 4.1.2).

(c) die Zertifizierung und die Konformitätszeichen nicht in einer Weise zu verwenden, die die Zertifizierungsstelle oder den Programmeigner in Misskredit bringen könnte sowie keinerlei Äußerungen über ihre Zertifizierung zu treffen, die die Zertifizierungsstelle oder der Programmeigner als irreführend oder unberechtigt betrachten könnte;

(d) bei Aussetzung, Einschränkung, Widerruf oder Beendigung der Zertifizierung die Verwendung aller Werbematerialien, die jeglichen Bezug auf die Zertifizierung enthalten, einzustellen und jeweils in diesem Programm geforderten Maßnahmen sowie alle weiteren von der Zertifizierungsstelle festgelegten Maßnahmen zu ergreifen;

(e) bei Bezugnahme auf ihre Zertifizierung in Kommunikationsmedien, wie z. B. Dokumenten, Broschüren oder Werbematerialien, die Anforderungen der Zertifizierungsstelle sowie die Anforderungen unter § 5.5.2 in Bezug auf die Verwendung von Konformitätszeichen festgelegt, zu erfüllen;

(f) Aufzeichnungen aller Beschwerden mindestens für die Gültigkeitsdauer der Zertifizierung aufzubewahren, die dem Cloud-Anbieter in Bezug auf die Einhaltung der Zertifizierungskriterien bekannt gemacht wurden und diese Aufzeichnungen der Zertifizierungsstelle und der zuständigen Datenschutzaufsichtsbehörde auf Anfrage zur Verfügung zu stellen; und

  (i) geeignete Maßnahmen zu ergreifen in Bezug auf solche Beschwerden sowie jegliche Mängel, die an den Datenverarbeitungsvorgängen entdeckt wurden und die die Einhaltung der Zertifizierungskriterien beeinflussen;

  (ii) die ergriffenen Maßnahmen zu dokumentieren.

(g) die Zertifizierungsstelle unverzüglich über Veränderungen zu informieren, die seine Fähigkeit, die Zertifizierungskriterien zu erfüllen, beeinträchtigen könnte (s. § 4.3.3, EDPB Annex 1 Tz. 4.1.2). Beispiele für Veränderungen sind unter § 4.3.3 genannt.

(h) dass Fristen und Verfahrensabläufe, die sich aus diesem Konformitätsbewertungsprogramm oder anderen Vorschriften ergeben, zwingend zu beachten und einzuhalten sind (s. DSK Tz 4.1.2.2);

(i) den Cloud-Nutzern auf Anfrage ausreichend Informationen über die beantragte Schutzklasse und Wiederherstellbarkeitsklasse, inkl. einer Begründung für die Auswahl der entsprechenden Schutz- bzw. Wiederherstellbarkeitsklasse, zur Verfügung zu stellen.

(17) Zertifizierungsstellen können für ihre Tätigkeit angemessene Entgelte verlangen. Die Entgelte sind in der Vereinbarung mit dem Cloud-Anbieter festzulegen. Der Cloud-Anbieter nimmt die für die ordnungsgemäße Zertifizierung erforderlichen bzw. ggf. vertraglich zugesagten Mitwirkungshandlungen auf eigene Kosten vor.

(18) Die erwartete Dauer des Zertifizierungsverfahrens wird zwischen den Beteiligten abgestimmt und in der Vereinbarung festgehalten (s. DSK Tz. 4.1.2.2).

(19) Wenn die Vereinbarung nach Beginn der Zertifizierungstätigkeiten geändert wird, muss die Vertragsprüfung nochmals durchgeführt werden. Jegliche Änderungen müssen allen betroffenen Personen, d.h. der Zertifizierungsstelle, ggf. ausgegliederten Evaluatoren und dem Cloud-Anbieter bekannt gemacht werden.

§ 5.1.3 Mitteilungspflichten des Cloud-Anbieters

(1) Die Zertifizierungsstelle fordert, dass der Cloud-Anbieter im Rahmen seiner Verantwortlichkeiten innerhalb der Datenverarbeitungsvorgänge sicherstellt, dass die Zertifizierungsstelle Zugriff auf zwingend notwendige Informationen und Daten und – insofern erforderlich – Zugang zu Datenverarbeitungsanlagen aller Art zur Durchführung der Zertifizierungstätigkeiten erhält.

(2) Die Zertifizierungsstelle fordert insbesondere vom Cloud-Anbieter folgende Informationen bereitzustellen (s. ISO/IEC 17065:2012 Tz. 7.2):

(a) der Wunsch gemäß dem AUDITOR-Kriterienkatalog und diesem Programm zertifiziert zu werden;

(b) die vom Cloud-Anbieter beantragte Schutzklasse und Wiederherstellbarkeitsklasse;

(c) Angaben zum Cloud-Anbieter, darunter Name und Anschrift(en der Standorte);

(d) allgemeine Informationen bezüglich des antragstellenden Cloud-Anbieters, die für den beantragten Zertifizierungsbereich relevant sind, wie z. B. seine Tätigkeiten, personelle

und technische Ressourcen, Organigramm, seine Marktausrichtung (national, EU, international, ausgewählte Märkte in Ländern etc.) und ggf. Beziehungen in einer größeren Körperschaft;

(e) eine umfassende Beschreibung des Zertifizierungsgegenstands gemäß § 5.1.4;
(f) eine umfassende Erläuterung zur Nichtanwendbarkeit von Zertifizierungskriterien gemäß § 5.1.5;
(g) eine umfassende Erläuterung zur Erfüllung der Zertifizierungskriterien gemäß § 5.1.6;
(h) ob Beratungsleistungen durch die Zertifizierungsstelle bezüglich des zu zertifizierenden Datenverarbeitungsvorgangs bereitgestellt wurden und falls ja, von wem und wann.

(3) Die Zertifizierungsstelle setzt dem Cloud-Anbieter eine angemessene Frist zur Übermittlung aller Informationen (in der Regel zwei bis drei Monate). Die Zertifizierungsstelle verpflichtet den Cloud-Anbieter alle Informationen fristgemäß entsprechend der im Zertifizierungsplan festgelegten Meilensteine, Fristen oder anderweitiger Zeitpunkte zur Verfügung zu stellen (s. EDPB Annex 1 Tz. 4.1.2).

(4) Im Verlaufe des Zertifizierungsverfahrens kann die Zertifizierungsstelle weitere, aus ihrer Sicht für die Zertifizierung notwendige Informationen und/oder Dokumentationen anfordern. Die Zertifizierungsstelle verpflichtet den Cloud-Anbieter diese Informationen bereitzustellen.

§ 5.1.4 Beschreibung und Festlegung des Zertifizierungsgegenstands

(1) Gegenstand der Bewertung (s. ISO/IEC 17000:2004 Tz. A.2.2) sind Datenverarbeitungsvorgänge von personenbezogenen Daten in Cloud-Diensten, s. hierzu § 2.2.8.

(2) Die Zertifizierungsstelle stellt sicher, dass der Cloud-Anbieter ausreichend Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstands zur Verfügung gestellt hat. Zudem muss der Cloud-Anbieter bei etwaigen Rückfragen zur Klärung von Unklarheiten beizutragen. Die vom Cloud-Anbieter bereitgestellte Dokumentation enthält mindestens eine detaillierte Beschreibung des Zertifizierungsgegenstands, dazu zählen

(a) die Benennung und detaillierte (Funktions-)Beschreibung des Datenverarbeitungsvorgangs oder der der Datenverarbeitungsvorgänge innerhalb eines entsprechenden Cloud-Dienstes, der zu zertifizieren ist;
(b) detaillierte Beschreibung aller Bestandteile der relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird;
(c) Dokumentation von Verantwortlichkeiten des Cloud-Anbieters im Datenverarbeitungsvorgang;
(d) Benennung und Informationen zu Standorten bei denen Datenverarbeitungsvorgänge durchgeführt werden (darunter Nennung Zentralstelle und weiterer Standorte und Beschreibung der Tätigkeiten, Risiken pro Standort, rechtliche und vertraglichen Regelungen für jeden Standort, den Grad der Zentralisierung der Prozesse/Tätigkeiten die für alle Standorten erbracht werden, die Schnittstellen zwischen den verschiedenen Standorten (s. IAF MD 1:2018 Tz. 7.1));
(e) Informationen bezüglich aller ausgegliederten Vorgänge, die von dem Cloud-Anbieter im Rahmen des Datenverarbeitungsvorgangs genutzt werden und welche die Konformität mit den Zertifizierungskriterien beeinflussen. Dabei müssen insbesondere Subauftragsverarbeiter und die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden (s. DSK Tz. 7.2);
(f) die Darstellung der Schnittstellen und Übergänge zu anderen Systemen und Organisationen/Subauftragsverarbeitern (bspw. in Form eines Netzplans). Hierbei sind auch die zugrundeliegenden Protokolle (bspw. Überwachungsprotokolle, (Muster-)Verträge, Vereinbarungen, Garantien) und sonstige Zusicherungen darzulegen (s. DSK Tz. 7.2);
(g) der TOM des Cloud-Anbieters i.S.d. Art. 28 DSGVO;
(h) eingesetzte Technik und IT-Landschaft, dazu zählen insbesondere relevante IT-Systeme;
(i) organisatorische Prozesse zur Durchführung der Datenverarbeitungsvorgänge;
(j) welche spezifischen Datenschutzrisiken die zu zertifizierenden Datenverarbeitungsvorgänge aufweisen.

(3) Die Zertifizierungsstelle dokumentiert die genaue Festlegung des Zertifizierungsgegenstandes und stellt diese dem Cloud-Anbieter zur Gegenprüfung zur Verfügung.

(4) Die Zertifizierungsstelle stellt auf Anfrage der Öffentlichkeit ausreichend Informationen über den Zertifizierungsgegenstand zur Verfügung, während gleichzeitig die Vertraulichkeit gewahrt wird. Ziel der Offenlegung ist die Schaffung von Transparenz bezüglich des konkreten Gegenstands der Bewertung, da Cloud-Dienste komplex sind.
(5) Die Zertifizierungsstelle und der Cloud-Anbieter können das Begleitdokument *‚AUDITOR-Zertifizierungsgegenstand‘* zur Unterstützung bei der Festlegung des Gegenstandes heranziehen.

§ 5.1.5 Nichtanwendbarkeit von Zertifizierungskriterien

(1) Die Zertifizierungsstelle fordert vom Cloud-Anbieter die Durchführung einer Prüfung zur Feststellung, welche Zertifizierungskriterien abhängig vom jeweiligen Zertifizierungsgegenstand anwendbar sind. Die Einschätzung der Nichtanwendbarkeit von Zertifizierungskriterien dokumentiert der Cloud-Anbieter und teilt diese der Zertifizierungsstelle mit. Die Dokumentation sollte dabei mindestens enthalten:

   (a) eine Auflistung der Kriterien, die nicht anwendbar sind;
   (b) eine ausführliche Begründung pro Kriterium, warum dieses für den konkreten Zertifizierungsgegenstand nicht anwendbar ist.

(2) Die Zertifizierungsstelle etabliert einen Prozess zur Bewertung und Dokumentation der Nichtanwendbarkeit von Zertifizierungskriterien. Dabei prüft die Zertifizierungsstelle die vom Cloud-Anbieter bereitgestellte Dokumentation zur Nichtanwendbarkeit auf Korrektheit und Vollständigkeit. Die Zertifizierungsstelle muss insbesondere sicherstellen, dass bei vergleichbaren Zertifizierungsverfahren und Sachverhalten die gleiche Entscheidung hinsichtlich der Nichtanwendbarkeit getroffen wird, um eine mögliche Willkür bei der Bewertung zu unterbinden.
(3) Wird die Nichtanwendbarkeit eins Kriteriums durch die Zertifizierungsstelle bestätigt, wird dieses Kriterium im Rahmen der Ermittlung nicht geprüft. Die Zertifizierungsstelle muss die nachweislichen Gründe, Entscheidungsregeln, sowie den Umfang der Nichtanwendbarkeit und die Ergebnisse der Bewertung dokumentieren.
(4) Bestehen Zweifel an der Nichtanwendbarkeit eins Kriteriums durch die Zertifizierungsstelle, wird eine Auflösung der Unklarheiten durch die Zertifizierungsstelle erwirkt. Hierzu können unter anderem weitere Dokumente und Erläuterungen vom Cloud-Anbieter angefordert werden oder Ermittlungsmethoden (s. § 5.2.4) durch die Zertifizierungsstelle angewendet werden.
(5) Nicht anwendbar sind Kriterien insbesondere dann, wenn

   (a) der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter bspw. nach dem Zertifizierungskriterium Nr. 6.2 zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt (bspw. im Falle eines Infrastructure-as-a-Service). Das Gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach dem Zertifizierungskriterium Nr. 2.3 verantwortlich sind. In diesem Fall ist das Zertifizierungskriterium Nr. 2.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (s. Zertifizierungskriterium Nr. 10.4) und somit ihrerseits das Zertifizierungskriterium Nr. 2.3 erfüllen.
   (b) die Erfüllung des Kriteriums verhindert, einen legitimen Datenverarbeitungszweck zu erreichen. So kann beispielsweise ein Anbieter eines E-Mail-Dienstes die Mailheader nicht anonymisieren, da ansonsten die Zustellung von E-Mails nicht mehr ordnungsgemäß gewährleistet werden kann, sodass er zu einer solchen Anonymisierung auch nicht verpflichtet werden kann.
   (c) der Cloud-Anbieter die in den Zertifizierungskriterien adressierten Handlungen nicht vornimmt. Setzt der Cloud-Anbieter bspw. keine Subauftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt, sind die Zertifizierungskriterien aus Kapitel V und VI des AUDITOR-Kriterienkatalogs nicht anwendbar.

(d) die Datenschutz-Grundverordnung oder die sie konkretisierenden Gesetze die Anwendbarkeit nicht absolut fordern, sondern von gewissen Voraussetzungen oder „Schwellen“ abhängig machen, welche vom Cloud-Anbieter nicht erfüllt werden. Dies ist beispielsweise bei der Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 und 4 DSGVO i.V.m. § 38 BDSG) oder beim Führen eines Verarbeitungsverzeichnisses der Fall (Art. 30 Abs. 5 DSGVO).

(6) Stellen der Cloud-Anbieter oder die Zertifizierungsstelle darüber hinaus (bspw. bei der Festlegung des Zertifizierungsgegenstands oder im Rahmen der Ermittlungs- und Bewertungstätigkeiten) eine Nichtanwendbarkeit von Zertifizierungskriterien aufgrund der besonderen Umstände und Eigenschaften des Datenverarbeitungsvorgangs fest, so ist diese ausführlich zu begründen und dazulegen.

§ 5.1.6 Stellungnahme zur Erfüllung der Zertifizierungskriterien

(1) Die Zertifizierungsstelle fordert vom Cloud-Anbieter eine detaillierte Stellungnahme zur Erfüllung der Zertifizierungskriterien, um eine nachfolgende Ermittlung vorbereiten und durchführen zu können.

(2) Eine Stellungnahme sollte dediziert für jedes Zertifizierungskriterium korrekt und vollständig darstellen, wie der Cloud-Anbieter das Kriterium umsetzt. Die Darstellung sollte dabei differenziert für die Unterpunkte des jeweiligen Kriteriums durchgeführt werden (bspw. Erläuterung zu Kriterium Nr. 2.2 (2)). Darüber hinaus kann die Darstellung eine Referenzierung zu der entsprechenden Dokumentation (bspw. Prozessdokumentation, Logs, Intranet, Wiki etc.) oder Systeme enthalten.

(3) Die Zertifizierungsstelle kann eine elektronische Vorlage zur Stellungnahme zur Unterstützung der Cloud-Anbieter anbieten.

(4) Der Cloud-Anbieter versichert gegenüber der Zertifizierungsstelle, dass die in der Stellungnahme genannten Maßnahmen vollständig umgesetzt sind.

§ 5.1.7 Anerkennung von bestehenden Zertifizierungen

(1) Wenn der Cloud-Anbieter eine Anerkennung bestehender Zertifizierungen für Bestandteile seiner Datenverarbeitungsvorgänge anstrebt, prüft die Zertifizierungsstelle unverzüglich, ob und inwieweit eine Anerkennung erfolgen kann.

(2) Es gibt nur drei Möglichkeiten im Rahmen des Zertifizierungsprozesses ein anderes Zertifikat als Teilevaluierung anzuerkennen (s. DSK Tz. 7.4, ISO/IEC 17065:2012 Tz. 6.2.2.4):

(a) Das Zertifikat wurde von einer akkreditierten Zertifizierungsstelle ausgestellt (bspw. ein ISO/IEC 27001 Zertifikat durch eine akkreditierte Zertifizierungsstelle);
(b) Das Zertifikat wurde von einer Stelle ausgestellt, die eine Begutachtung unter Gleichrangigen durchlaufen hat (gem. ISO/IEC 17040:2005);
(c) Das Zertifikat wurde durch eine staatliche Zertifizierungsstelle auf gesetzlicher Grundlage ausgestellt (z.B. Cyber Security Act).

(3) Notwendig für eine Bewertung der Anerkennung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens (bspw. Auditreport). Insofern dies nicht möglich ist (bspw. keine Weitergabe der Dokumente aus rechtlichen oder vertraglichen Gründen möglich), muss der Cloud-Anbieter ausreichende Informationen bereitstellen, die eine Bewertung der Zertifizierung ermöglichen (s. DSK Tz. 7.4, EDPB Annex 1 Tz. 7.4). Eine Zertifizierungsurkunde oder ähnliche Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend.

(4) Ferner müssen die Unterlagen zur bestehenden Zertifizierung einen genau beschriebenen Zertifizierungsgegenstand und eine Darstellung der Schnittstellen bzw. Übergänge zu anderen Systemen und Organisationen enthalten (bspw. ISO/IEC 27001 Statement of Applicability, SoA).

(5) Der zu zertifizierende Datenverarbeitungsvorgang muss Bestandteil des Geltungsbereichs der bestehenden Zertifizierung sein (bspw. Datenverarbeitungsvorgang ist Bestandteil des nach ISO/IEC 27001 zertifizierten ISMS).

(6) Die anzuerkennenden Evaluierungen der Zertifizierungen müssen vor Antragstellung des Cloud-Anbieters abgeschlossen sein (s. DSK Tz. 7.4).

(7) Soweit die Zertifizierungsstelle Zertifikate für Bestandteile von Datenverarbeitungsvorgängen anerkennt, ist eine vollständige Bewertung des im Zertifikat benannten Bestandteils des Datenverarbeitungsvorgangs nicht erforderlich. Die Zertifizierungsstelle ist jedoch weiterhin verpflichtet die aktuelle Einhaltung der Kriterien (der vorgelegten Zertifizierung) zumindest stichprobenartig zu überprüfen und bestehende Zertifizierungen zu bewerten.

(8) Erforderlich ist zudem eine Bewertung des Zusammenwirkens des anerkannten Bestandteils des Datenverarbeitungsvorgangs mit anderen Bestandteilen, insbesondere der für dieses Zusammenwirken maßgeblichen Schnittstellen.
(9) Ergeben sich im Rahmen der AUDITOR-Zertifizierung Unregelmäßigkeiten in Hinblick auf anerkannte Zertifizierungen (bspw. Vermutung von Abweichungen), so ist die Ermittlung im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. auf den gesamten, bereits zertifizierten Gegenstand auszudehnen (s. DSK Tz. 7.4, EDPB Annex 1 Tz. 7.4).
(10) Die Zertifizierungsstelle hat die Anerkennung, insbesondere hinsichtlich der Schutzklasse und der Wiederherstellbarkeitsklasse, zu begründen und ausreichend zu dokumentieren. Insbesondere muss dokumentiert werden, wie und in welchem Umfang dies der Fall ist und welche Auswirkungen dies konkret auf den verbleibenden Ermittlungsumfang und die Ermittlungsmethoden hat (s. DSK Tz. 7.4).
(11) Die Zertifizierungsstelle notiert die Gültigkeit und Befristung der anerkannten Zertifikate und hält diese für die Entscheidung vor (s. § 5.5.5). Die fortlaufende Gültigkeit der anerkannten Zertifikate wird mindestens im Rahmen der Überwachungsaudits von der Zertifizierungsstelle überprüft. Darüber hinaus verpflichtet die Zertifizierungsstelle den Cloud-Anbieter, diese mit ausreichend Vorlaufzeit darüber in Kenntnis zu setzen, wenn ein anerkanntes Zertifikat die Gültigkeit planmäßig verliert (d.h. bei regulärem Ablauf des Gültigkeitszeitraums) oder außerplanmäßig verliert (d.h. vor dem von der Zertifizierungsstelle vermerkten Ende des regulären Gültigkeitszeitraum), und welche Maßnahmen der Cloud-Anbieter vornehmen will (bspw. Rezertifizierung). Strebt der Cloud-Anbieter keine Rezertifizierung des anerkannten Zertifikats an, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der AUDITOR-Zertifizierung aufrecht zu erhalten.
(12) Bei der Prüfung der Anerkennung muss die materielle und verfahrensmäßige Gleichwertigkeit der Ergebnisse von Konformitätsbewertungen sichergestellt werden, um ein gleiches Niveau des Vertrauens in die Konformität sicherzustellen (s. DSK Tz. 7.4, ISO/IEC 17000:2004 Tz. 7.4):

   (a) Eine materielle Gleichwertigkeit liegt vor, wenn das andere Zertifikat auf Zertifizierungskriterien beruht, die denen des AUDITOR-Kriterienkatalogs im Hinblick auf das Schutzniveau vergleichbar sind oder diese übertreffen. Die Zertifizierungsstelle stellt insbesondere fest, mit welcher Schutzklasse und welcher Wiederherstellbarkeitsklasse das Zertifikat anerkannt wird.
   (b) Eine verfahrensmäßige Gleichwertigkeit liegt vor, wenn das andere Zertifikat in einem akkreditierten Zertifizierungsverfahren erteilt wurde, das eine dieser Verfahrensordnung vergleichbare Gewähr für die ordnungsgemäße Prüfung und Zertifizierung bietet.

   In der Regel liegt eine Gleichwertigkeit bei Zertifikaten vor, welche durch eine akkreditierte Zertifizierungsstelle vergeben werden, und somit insbesondere bei bewilligten Datenschutzzertifizierungen nach Art. 43 DSGVO.
(13) Auswirkungen auf die Gültigkeitsdauer der eingebrachten Zertifizierung ergeben sich nicht.
(14) Andere erteilte Zertifizierungen können im Rahmen der Zertifizierung nicht anerkannt werden. Andere Zertifizierungen und deren Ergebnisberichte können lediglich vom Cloud-Anbieter vorgelegt und von der Zertifizierungsstelle bei Bedarf im Rahmen ihrer Ermittlungstätigkeiten im Sinne einer Dokumentprüfung miteinbezogen werden. Die Einhaltung der Zertifizierungskriterien muss jedoch von der Zertifizierungsstelle durch weitere geeignete Ermittlungsmethoden vollumfänglich überprüft werden.
(15) Weitere Informationen bietet auch das Begleitdokument *‚AUDITOR-Modularitätskonzept‘*.

§ 5.1.8 Bewertung der zur Verfügung gestellten Informationen und Dokumentationen

(1) Die Zertifizierungsstelle muss eine Bewertung der erhaltenen Informationen vornehmen (allgemein bekannt als „Stage 1 Prüfung“), um sicherzustellen, dass (s. ISO/IEC 17065:2012 Tz. 7.3.1):

   (a) die Informationen über den Cloud-Anbieter und den Datenverarbeitungsvorgang ausreichend für die Durchführung des Zertifizierungsprozesses sind;
   (b) die Zertifizierungsstelle ein ausreichendes Verständnis über den Datenverarbeitungsvorgang erlangen konnte;
   (c) alle bekannten Differenzen im Verständnis zwischen der Zertifizierungsstelle und dem Cloud-Anbieter geklärt wurden;

(d) der Zertifizierungsgegenstand und Geltungsbereich der angestrebten Zertifizierung festgelegt ist;
(e) die Mittel zur Durchführung aller Auswahl- und Ermittlungstätigkeiten verfügbar sind;
(f) die Zertifizierungsstelle über die technische und juristische Kompetenz und die Fähigkeit verfügt, die angeforderten Zertifizierungstätigkeiten für den individuellen Zertifizierungsgegenstand des Cloud-Anbieters durchzuführen. Bei fehlender Erfahrung mit dem Zertifizierungsgegenstand oder dem Cloud-Dienst-Typ muss die Zertifizierungsstelle sowohl eine technische als auch rechtliche Kompetenz in angemessenem Umfang für die Zertifizierungstätigkeiten des Einzelauftrages darlegen (s. DSK Tz. 7.3, EDPB Annex 1 Tz. 7.3).

(2) Die Zertifizierungsstelle macht den Cloud-Anbieter auf die weiteren Arten von Informationen und Aufzeichnungen aufmerksam, die für eine detaillierte Ermittlung gemäß Kapitel Nr. 5.2 erforderlich sein können (allgemein bekannt als „Stage 2 Prüfung“).
(3) In dem Fall, dass Informationen nicht der Zertifizierungsstelle zur Verfügung gestellt werden können, weil sie vertrauliche oder sensible Informationen enthalten, bestimmt die Zertifizierungsstelle, ob der Datenverarbeitungsvorgang dennoch angemessen geprüft werden kann. Wenn die Zertifizierungsstelle zu dem Schluss kommt, dass es nicht möglich ist, den Datenverarbeitungsvorgang angemessen zu prüfen, ohne die identifizierten vertraulichen oder sensiblen Informationen zu überprüfen, weist sie den Cloud-Anbieter darauf hin, dass das Zertifizierungsverfahren erst fortgeführt werden kann, wenn eine geeignete Zugangsvereinbarung getroffen wurde.
(4) Die Zertifizierungsstelle hat das Recht, das Zertifizierungsverfahren auszusetzten oder abzubrechen, sofern der Cloud-Anbieter der Pflicht zur Beibringung dieser Informationen und/oder Dokumentationen nicht nachkommt (s. DSK Tz. 7.4).

5.2 Ermittlung

§ 5.2.1 Ermittlung des Zeitaufwandes

(1) Die Zertifizierungsstelle muss dokumentierte Verfahren zur Ermittlung des Ermittlungszeitaufwandes haben (s. ISO/IEC 17065:2013 Tz. 7.4.1). Insbesondere muss die Zertifizierungsstelle für jeden Cloud-Anbieter den Zeitaufwand ermitteln, der benötigt wird, um eine vollständige und wirksame Ermittlung planen und durchführen zu können.
(2) Die Ermittlungszeit sollte möglichst gering sein, um auch die Zertifizierung von kleinen und mittelständigen Cloud-Anbietern zu ermöglichen (i.S.d. Art. 42 Abs. 1 DSGVO). Gleichzeitig müssen ein möglichst hoher Prüfumfang und eine ausreichende Prüftiefe erreicht werden, um die die Schutzaussage der AUDITOR-Zertifizierung und die Einhaltung der Anforderungen der Datenschutz-Grundverordnung sicherzustellen.
(3) Die Dauer der Ermittlung sowie ihre Rechtfertigung müssen aufgezeichnet werden.
(4) Die festgelegte Ermittlungszeit kann verlängert werden, insofern bspw. im Rahmen der Ermittlung besondere Feststellungen gemacht wurden (bspw. Prüfung weiterer Standorte, andere Komplexität des Datenverarbeitungsvorgangs als ursprünglich geplant) oder Nachprüfungen erforderlich sind.
(5) Zur Ermittlung des Zeitaufwands gibt Anhang A: Festlegung der Ermittlungszeit verbindliche Vorgaben.

§ 5.2.2 Planen der Ermittlung

(1) Die Evaluatoren fertigen vor der Durchführung der Ermittlung einen Ermittlungsplan an (s. ISO/IEC 17065:2012 Tz. 7.4.1), welcher mindestens Angaben zum zeitlichen Ablauf sowie der anzuwenden Ermittlungsmethoden umfasst. Der Ermittlungsplan ist dem Cloud-Anbieter auszuhändigen.
(2) Die Zertifizierungsstelle muss Personal zur Durchführung jeder Ermittlungsaufgabe, die sie mit ihren internen Ressourcen ausführt, benennen (s. ISO/IEC 17065:2012 Tz. 7.4.2).

§ 5.2.3 Ermittlungsobjekte

(1) Die Ermittlung erfolgt auf Grundlage der im Auftrag klar abgegrenzten Beschreibung des Zertifizierungsgegenstands. Der gesamte Zertifizierungsgegenstand, inklusive aller technischen und organisatorischen Vorgänge oder Vorgangsreihen, muss den anwendbaren Zertifizierungskriterien des AUDITOR-Kriterienkatalogs in der maßgeblichen Fassung entsprechen.
(2) Gegenstand der Ermittlung ist auch das Zusammenwirken der Datenverarbeitungsvorgänge oder deren Bestandteile mit anderen Bestandteilen, Datenverarbeitungsvorgängen oder

Diensten. Hierzu zählt insbesondere auch die Betrachtung möglicher Schnittstellen zu Subauftragsverarbeitern.

(3) Zur Feststellung der Konformität mit den Zertifizierungskriterien des AUDITOR-Kriterienkatalogs können unterschiedliche Ermittlungsobjekte begutachtet werden. Dabei setzt sich ein Cloud-Dienst aus einem oder mehreren Datenverarbeitungsvorgängen zusammen. Einem Datenverarbeitungsvorgang können wiederrum Ermittlungsobjekte zugeordnet werden, darunter Vereinbarungen (4), Prozesse (5), Anbietereigenschaften (6), Diensteigenschaften (7), Infrastrukturkomponenten (8), Softwarekomponenten (9), die Entwicklungsumgebung (10), Mitarbeiter des Cloud-Anbieters (11), und (12) das (Datenschutz-)Managementsystem.

(4) Bei rechtsverbindlichen Vereinbarungen als Ermittlungsobjekt werden die Eigenschaften und Inhalte von Verträgen oder Vereinbarungen mit Cloud-Nutzern oder Subauftragsverarbeitern bewertet.

(5) Ein Prozess oder eine entsprechende und realitätsnahe Prozessdokumentation kann überprüft werden, um die Konformität mit den Zertifizierungskriterien zu bestätigen.

(6) Eine Prüfung von Anbietereigenschaften umfasst die Begutachtung von Eigenschaften und Ausprägungen des Cloud-Anbieters, bspw. die zugrundeliegende Organisationsstruktur.

(7) Zu den Diensteigenschaften gehören insbesondere Cloud-Dienst-Features und -Funktionen, die für den Cloud-Nutzer unmittelbar sichtbar sind und überprüft werden müssen.

(8) Eine Überprüfung kann Infrastrukturkomponenten umfassen, also physische Objekte, wie bspw. Hardware-Komponenten oder die Rechenzentrumsinfrastruktur.

(9) Die Prüfung von Softwarekomponenten umfasst virtuelle Objekte, bspw. Quellcode sowie die Zusammenstellung und Interaktionen der einzelnen Komponenten der Datenverarbeitungsvorgänge.

(10) Die Prüfung der Entwicklungsumgebung umfasst eingesetzte Entwicklungsmethoden, sichere und vom Produktivsystem getrennte Test- und Entwicklungsumgebung, und Abnahmetests.

(11) Die Prüfung von Mitarbeitern kann notwendig sein, um bspw. deren fachliche oder persönliche Eignung sicherzustellen.

(12) Die Prüfung des (Datenschutz-)Managementsystems ist notwendig, um zu erkennen, ob der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System umgesetzt hat, das im Einklang mit der Politik der Organisation und den Zertifizierungskriterien steht.

§ 5.2.4 Ermittlungsmethoden

(1) Die Ermittlungen müssen unparteilich durchgeführt werden und derart strukturiert und gehandhabt werden, dass die Unparteilichkeit sichergestellt ist (s. ISO/IEC 17065:2012 Tz. 4.2). Die Evaluatoren dürfen keinen kommerziellen, finanziellen oder sonstigen Druck zulassen, der die Unparteilichkeit gefährdet.

(2) Die Ermittlung (allgemein bekannt als „Stage 2 Prüfung“) umfasst abhängig vom Zertifizierungskriterium eine Prüfung der vom Cloud-Anbieter zur Verfügung gestellten Dokumentationen (3), Inspektionen (4), Prüfungen (5), Audits (6), und/oder Entwicklungs- und Designprüfungen (7).

(3) Dokumentprüfung. Mit der Dokumentprüfung überprüft der Evaluator die Einhaltung der Zertifizierungskriterien anhand der Angaben in der Dokumentation des Cloud-Anbieters. Ein Cloud-Anbieter legt entsprechende Dokumente, (technische) Logs, Testate oder andere Dokumentationen vor. Insbesondere findet hierbei eine Rechtsanalyse statt (bspw. der rechtsverbindlichen Vereinbarungen), um sicherzugehen, dass die geltenden rechtlichen Kriterien erfüllt werden. Zudem können im Rahmen einer Dokumentprüfung auch Personenzertifikate (im Sinne der ISO/IEC 17024) zum Kompetenznachweis für das Personal bzw. einer natürlichen Person (bspw. des Datenschutzbeauftragten) und zur Gewährleistung eines angemessenen Datenschutzniveaus überprüft werden. Eine Dokumentprüfung ist stets mit geeigneten Ermittlungsmethoden zu ergänzen, um sicherzustellen, dass die dokumentierten Anweisungen, Verfahren, Regeln etc. auch fortlaufend vom Cloud-Anbieter umgesetzt werden.

(4) Inspektion (im Sinne der ISO/IEC 17020). Im Rahmen einer Inspektion wird die Konformität eines Produktes oder Prozesses mit spezifischen Anforderungen (hier DSGVO und den Zertifizierungskriterien) untersucht. Inspektionsparameter schließen Fragen zur Quantität, Qualität, Sicherheit, Zweckmäßigkeit sowie fortdauernden Einhaltung der Sicherheit von in Betrieb befindlichen Anlagen oder Systemen ein. In Bezug auf die AUDITOR-Datenschutzzertifizierung wird mittels einer (rechtlichen) Inspektion insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO

überprüft. Die Inspektion kann alle Phasen im Rahmen der Lebensdauer der Ermittlungsobjekte betreffen, einschließlich der Entwicklungsphase. Bei der Inspektion können bspw. Datenverarbeitungsvorgänge im Rahmen einer Dienstnutzung durchgeführt werden, um die Funktionsweise und die Ergebnisse der Vorgänge beurteilen zu können. Ein Evaluator vergleicht hierbei die zu erwartenden Ergebnisse gemäß der vorliegenden Dokumentation mit den tatsächlichen Ergebnissen, welche durch eine Dienstnutzung erbracht werden. Er erhält somit keinen Einblick in die internen Verarbeitungsschritte der Verarbeitungsvorgänge (‚Black-Box-Test'). Daneben kann ein Vorgang oder eine Vorgangsreihe auch angestoßen und die tatsächliche Ausführung überwacht (‚monitoring') oder Logs der Vorgangsausführung überprüft werden (‚White-Box-Test').

(5) Prüfung (im Sinne der ISO/IEC 17025:2017). Eine Prüfung umfasst Tests oder Messungen zur Untersuchung des Datenverarbeitungsvorgangs bzw. des Ermittlungsobjektes und zur Feststellung ihrer Übereinstimmung mit den Zertifizierungskriterien. So kann eine Assetprüfung durchgeführt werden, indem bei der Prüfung ein Asset (z.B. Hardware oder Softwarecode und ggf. die dazugehörige Dokumentation) untersucht wird. Die Prüfung kann in Begleitung oder unter Anweisung eines Mitarbeiters des Cloud-Anbieters oder eigenständig durch den Evaluator durchgeführt werden. Der Cloud-Anbieter ist vorab über die Prüfung zu informieren und stellt den Evaluator bspw. notwendige Zugänge (bspw. Test-Accounts) oder (technische) Logs über die Ausführung des Vorgangs zur Durchführung der Prüfung bereit. Insofern notwendig, wählt der Evaluator geeignete Testdaten. Hierzu zählen zufällig erzeugte Werte, die eine realistische und funktionskonforme Prüfung des Vorgangs ermöglichen. Ein Evaluator kann zur Prüfung und Überwachung des Vorgangs (‚monitoring') geeignete (ggf. extern bereitgestellte) Testierungs- und Auditierungsprodukte und -dienstleistungen nutzen (s. ISO/IEC 17025:2017 Tz. 6.6). Die eingesetzten Produkte und Dienstleistungen zur Prüfung sind im Ermittlungsbericht zu dokumentieren. Bei invasiven Ermittlungsverfahren oder Verfahren, die zu einer Beeinträchtigung von Datenverarbeitungsvorgängen des Cloud-Dienstes führen könnten, ist eine Abstimmung mit dem Cloud-Anbieter notwendig. Der Cloud-Anbieter ist verpflichtet den Evaluator bei der Durchführung zu unterstützen. In Bezug auf die AUDITOR-Datenschutzzertifizierung wird mittels einer (rechtlichen) Prüfung insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO überprüft. Bspw. kann mittels Sicherheitstests die korrekte und starke Verschlüsselung von Daten festgestellt werden. Bei der Durchführung von Sicherheitstests sei weiterführend auf die ISO/IEC 15408:2009 und ISO/IEC 18045:2008-018 hingewiesen.

(6) Audit (im Sinne der ISO/IEC 17021-1:2015). Ein Audit wird zum Zweck der Zertifizierung des (Datenschutz-)Managementsystems des Cloud-Anbieters durchgeführt (s. ISO/IEC 17021-1:2015 Tz. 3.4), um zu erkennen, dass der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System verwendet, das im Einklang mit der Politik der Organisation sowie den Zertifizierungskriterien steht. Audits können vor Ort, aus der Ferne oder in einer Kombination aus beidem durchgeführt werden (s. ISO 19011:2018-10 Tz 5.5.3). Der Einsatz dieser Methoden sollte angemessen ausgewogen sein, unter anderem auf Grundlage der Berücksichtigung der damit verbundenen Risiken und Chancen. Im Rahmen des Audits können insbesondere Befragungen, Beobachtungen und Prüfungen durchgeführt werden, um Informationen über Wissen und Fertigkeiten zu ermitteln sowie festzustellen, ob Prozesse und das Managementsystem beim Cloud-Anbieter gelebt werden. Die Befragung von Mitarbeitern des Cloud-Anbieters oder anderen Personen, die mit der Erbringung der Datenverarbeitungsvorgänge befasst sind, kann zur Sachverhaltsermittlung einzelner Aspekte und zur Überprüfung der Richtigkeit der Dokumentation eingesetzt werden (s. ISO/IEC 17021-1:2015 Tz. B.4). Sie soll insbesondere zur Überprüfung bei vom Evaluator als kritisch erkannten Aspekten eingesetzt werden. Befragungen können schriftlich oder persönlich durchgeführt werden. Sie sollen jedenfalls hinsichtlich zentraler Aspekte als mündliche Befragung durchgeführt werden. Soweit eine persönliche Befragung unverhältnismäßig wäre, kann sie in Form von Videokonferenzen durchgeführt werden. Eine Person bei der Erfüllung einer Aufgabe zu beobachten, kann durch die damit dargelegte Anwendung von Wissen und Fertigkeiten zur Erzielung eines gewünschten Ergebnisses direkte Nachweise für die Kompetenz liefern (s. ISO/IEC 17021-1:2015 Tz. B.5). Schriftliche, mündliche und praktische Prüfungen können gute und gut dokumentierte Nachweise für vorhandenes Wissen und — je nach angewendeter Methodik — auch für Fertigkeiten liefern (s. ISO/IEC 17021-1:2015 Tz. B.6). Eine Vor-Ort-Prüfung umfasst die Inaugenscheinnahme der Verfahren und technischen Einrichtungen in den Räumlichkeiten des Cloud-Anbieters. In Bezug auf die AUDITOR-Datenschutzzertifizierung sollen insbesondere (rechtliche) Audits durchgeführt wer-

den, um eine korrekte Einrichtung, Aufrechterhaltung und Pflege eines Datenschutz-Managementsystems (im Sinne von Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO) zu prüfen. Die Sicherstellung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen. Für weiterführende Literatur zur Durchführung von Audits sei insbesondere auf die ISO/IEC 17021-1:2015 Tz. 9.4 und ISO 19011:2018-10 verwiesen. Für die Durchführung von Audits aus der Ferne sei auf IAF MD 4:2018 verwiesen.

(7) Entwicklungs- und Designprüfung. Eine Entwicklungsprüfung umfasst die Prüfung von Entwicklungsmethoden und -verfahren sowie bei Bedarf eine Prüfung der Testsysteme und -umgebungen, welche bei der Entwicklung von Hard- und Software zur Erbringung der Datenverarbeitungsvorgänge eingesetzt werden. Bei der Designprüfung können unter anderem die gewählte Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs überprüft werden. Eine Entwicklungs- und Designprüfung sollte auch eine Rechtsanalyse umfassen, um sicherzugehen das die geltenden rechtlichen Kriterien erfüllt werden. So kann eine rechtliche Entwicklungs- und Designprüfung insbesondere im Rahmen der Prüfung zur Erfüllung des Art. 25 DSGVO oder zur Überprüfung der Datenschutz-Folgenabschätzung erforderlich sein.

(8) Die anzuwendenden Ermittlungsmethoden sind im Begleitdokument *‚AUDITOR-Ermittlungsmethoden‘* für jedes Zertifizierungskriterium spezifiziert und entsprechend durch die Evaluatoren anzuwenden.

(9) Ermittlungsmethoden können bei Bedarf kombiniert werden, um (zusätzliche) fundierte Informationen über das Ermittlungsobjekt zu erheben.

(10) Die Ermittlung kann gemäß § 5.2.5 stichprobenartig erfolgen.

(11) Bei der Ermittlung müssen die relevanten internationalen Normen zur Ermittlungsart berücksichtigt werden. Die relevanten internationalen Normen sind für die Prüfung ISO/IEC 17025, für die Inspektion ISO/IEC 17020, für die Durchführung von Audits von Managementsystemen ISO/IEC 17021 und für Personenzertifizierungen ISO/IEC 17024. Ferner sei auf das *„Merkblatt zu Akkreditierungsverfahren im Datenschutz“* hingewiesen.

(12) Ein Evaluator muss sicherstellen, dass nicht nur eine ausreichende Dokumentation als Nachweis vorliegt, sondern auch, dass die dokumentierten Maßnahmen umgesetzt und fortlaufend vom Cloud-Anbieter und dessen Mitarbeitern ‚gelebt‘ werden. Insbesondere bei Ermittlungstätigkeiten im Rahmen der AUDITOR-Datenschutzzertifizierung sollte eine fortlaufende Rechtsanalyse durchgeführt werden. So soll bspw. im Rahmen einer Dokumentprüfung nicht nur die Prüfung von Vereinbarungen, sondern vor allem auch durch geeignete weitere Ermittlungsmethoden die konkrete Umsetzung beim Cloud-Anbieter als Auftragsverarbeiter überprüft werden, um sicherzugehen das die geltenden rechtlichen Kriterien erfüllt werden.

(13) Die Zertifizierungsstelle muss ein Verfahren zur Sicherstellung der Integrität und Verlässlichkeit bei der Informationssammlung für die Ermittlung etablieren. Insbesondere bei der Bereitstellung von Informationen und Daten durch den Cloud-Anbieter, ist dazulegen, wie die Integrität dieser Informationen und Daten durch konkrete Verifikation oder sonstige Kontrollen der Zertifizierungsstelle sichergestellt werden kann.

(14) Die Ausführung von einzelnen Ermittlungstätigkeiten ist zu protokollieren. Die Aufzeichnungen müssen das Datum und die Identität der Personen beinhalten, die für die jeweiligen Ermittlungstätigkeiten verantwortlich sind. Beobachtungen, Daten und Berechnungen müssen zu dem Zeitpunkt, zu dem sie gemacht werden, aufgezeichnet werden und der speziellen Ermittlungstätigkeiten zugeordnet werden. Änderungen an den Aufzeichnungen zu früheren Versionen oder zu ursprünglichen Beobachtungen müssen zurückverfolgt werden können.

(15) Ermittlungsergebnisse und prüfungsrelevante Aufzeichnungen müssen vor unbefugtem Zugriff geschützt und gegen Manipulation und Verlust gesichert sein.

§ 5.2.5 Wahl von Strichproben bei der Ermittlung

(1) Eine Stichprobenentnahme findet dann statt, wenn es weder praktikabel noch kostengünstig ist, alle verfügbaren Informationen während einer Ermittlung zu prüfen (s. ISO 10911:2018 Tz. A.6.1). So können bspw. die Aufzeichnungen zu zahlreich oder geographisch zu weit gestreut sein, um eine Prüfung jedes einzelnen Elements der Grundgesamtheit zu rechtfertigen. Stichprobenentnahme bei der Ermittlung aus einer großen Grundgesamtheit ist der Prozess der Auswahl von weniger als 100 % der Einheiten innerhalb der insgesamt zur Verfügung stehenden Datenmenge (Grundgesamtheit), um Erkenntnisse über ein Merkmal dieser Grundgesamtheit zu erhalten und zu bewerten mit dem Ziel, eine Schlussfolgerung hinsichtlich der Grundgesamtheit ziehen zu können.

(2) Die Stichprobenentnahme umfasst folgende Schritte (s. ISO 10911:2018 Tz. A.6.1):

(a) Festlegen der Ziele der Stichprobenentnahme;
(b) Auswahl des Ausmaßes sowie der Zusammensetzung der Grundgesamtheit, aus der Proben zu entnehmen sind;
(c) Auswahl einer Methode zur Stichprobenentnahme;
(d) Bestimmen der Größe der zu entnehmenden Stichprobe;
(e) Durchführen der Probenentnahmetätigkeit;
(f) Zusammenstellen, Beurteilen, Berichten und Dokumentieren der Ergebnisse.

(3) Die Auswahl einer geeigneten Stichprobe sollte sich sowohl auf das Probenentnahmeverfahren als auch auf die Art der geforderten Daten stützen, z. B. um ein bestimmtes Verhaltensmuster abzuleiten oder Schlüsse über eine Grundgesamtheit zu ziehen (s. ISO 10911:2018 Tz. A.6.1).

(4) Die Stichprobe ist mindestens so umfassend zu wählen, dass die Untersuchung der ausgewählten Proben einen Rückschluss auf die Erfüllung der Zertifizierungskriterien zulässt. Die Zertifizierungsstelle muss sicherstellen, dass eine genommene Probe die Grundgesamtheit repräsentiert.

(a) In der Regel wird eine Stichprobengröße von 3% als repräsentativ angesehen.
(b) Auf die Wirtschaftlichkeit bei der Stichprobenwahl ist zu achten, um auch kleinen und mittelständigen Cloud-Anbietern die Zertifizierung zu ermöglichen. Aus diesem Grund kann bei einer sehr großen Grundgesamtheit (bspw. bei der Prüfung von rechtsverbindlichen Vereinbarungen) auch in Ausnahmen die folgende Formel verwendet werden:
$y = \lceil (\sqrt[2,5]{x}) \rceil$.
Der Umfang der Stichprobe muss die 2,5-Wurzel der Grundgesamtheit sein, gerundet auf die höhere ganze Zahl, wobei y = die Anzahl an Objekten ist, die in die Stichprobe aufzunehmen sind und x = die Gesamtanzahl an Objekten.
Beispiel: bei 1000 geschlossenen rechtsverbindlichen Vereinbarungen sollten 16 Vereinbarungen in die Stichprobe aufgenommen und überprüft werden.

(5) Bei der Probeentnahme sollten sowohl technische als auch organisatorische Ermittlungsobjekte einbezogen werden, insofern diese von den Zertifizierungskriterien betroffen sei könnten.

(6) Bei der Stichprobenentnahme sollte die Qualität der verfügbaren Daten berücksichtigt werden, da Probenentnahmen aus unzureichenden und ungenauen Daten kein brauchbares Ergebnis liefern (s. ISO 10911:2018 Tz. A.6.1).

(7) Es können entweder die entscheidungsbasierte Stichprobenentnahme oder die statistische Stichprobenentnahme angewandt werden.

(8) *Entscheidungsbasierte Stichprobenentnahme* (s. ISO 10911:2018 Tz. A.6.2): Entscheidungsbasierte Stichprobenentnahme stützt sich bei der Festlegung von Proben auf Kompetenz und Erfahrungen der Evaluatoren. Bei der entscheidungsbasierten Stichprobenentnahme sollte Folgendes durch den Evaluator berücksichtigt werden:

(a) frühere Ermittlungserfahrungen bei vergleichbaren Zertifizierungsverfahren und Zertifizierungsgegenständen;
(b) Anforderungen und Komplexität der Zertifizierungskriterien für die eine Probe genommen werden soll;
(c) Komplexität des Ermittlungsobjektes und vorliegende Wechselwirkungen (bspw. mit anderen Vorgängen);
(d) Grad der Veränderung und Vielfältigkeit des Ermittlungsobjektes in Bezug auf die Technik, den menschlichen Faktor oder das Datenschutz-Managementsystem;
(e) mögliche Risiken, die das Ermittlungsobjekt betreffen oder dem Zertifizierungskriterium inne sind;
(f) Ergebnisse aus Überwachungstätigkeiten oder vorangegangenen Ermittlungen.

(9) *Statistische Stichprobenentnahme* (s. ISO 10911:2018 Tz. A.6.2): Statistische Verfahren zur Stichprobenentnahme verwenden ein Probeauswahlverfahren, das auf Wahrscheinlichkeitstheorie beruht. Stichprobenprüfungen anhand der Anzahl fehlerhafter Einheiten (Attributprüfungen) werden verwendet, wenn es nur zwei mögliche Ergebnisse bei jeder Stichprobe gibt (z. B. richtig/falsch oder bestanden/nicht bestanden). Stichprobenprüfungen anhand quantitativer Merkmale (Variablenprüfungen) werden verwendet, wenn die Ergebnisse der Stichproben in einem kontinuierlichen Bereich auftreten. Der Plan zur Stichprobenentnahme sollte

berücksichtigen, ob die Ergebnisse, die geprüft werden, wahrscheinlich attributbasiert oder variablenbasiert sind. Bspw. könnte bei der Beurteilung der Konformität abgeschlossener Vereinbarungen mit den Zertifizierungskriterien ein attributbasierter Ansatz verwendet werden. Bei der Prüfung der Anzahl der Sicherheitsverstöße würde ein variablenbasierter Ansatz wahrscheinlich besser geeignet sein. Elemente, die einen Einfluss auf die Stichprobenentnahme haben können und daher beachtet werden müssen, sind:

(a) Kontext, Größe, Art und Komplexität des Ermittlungsobjektes sowie mögliche Wechselwirkungen;
(b) Anforderungen und Komplexität der Zertifizierungskriterien für die eine Probe genommen werden soll;
(c) die Häufigkeit der Stichprobenentnahme;
(d) der Zeitpunkt der Stichprobenentnahme;
(e) das gewählte Vertrauensniveau, in der Regel sollte das Probenentnahmerisiko nicht größer als 5% sein. Ein Probenentnahmerisiko von 5 % bedeutet, dass der Evaluator bereit ist, das Risiko zu akzeptieren, dass 5 von 100 der geprüften Proben nicht die tatsächlichen Werte widerspiegeln, die sich ergeben würden, wenn die Grundgesamtheit geprüft worden wäre;
(f) das Auftreten von unerwünschten und/oder unerwarteten Ereignissen.

(10) Die Evaluatoren müssen Aufzeichnungen der Daten zur Probenentnahme aufbewahren, die Teil der durchzuführenden Ermittlung sind. Diese Aufzeichnungen müssen, wo zutreffend, Folgendes enthalten:

(a) einen Verweis auf das angewandte Probenentnahmeverfahren und etwaige Probenentnahmekriterien, die für die Beurteilung verwendet wurden (z. B. was eine annehmbare Stichprobe ist);
(b) das Datum der Probenentnahme;
(c) eine Begründung für Probennahme;
(d) das Ermittlungsobjekt für das eine Stichprobe genommen wird;
(e) Beschreibung der Grundgesamtheit;
(f) Daten zur Identifizierung und Beschreibung der Probe (z. B. Größe, Nummer, Menge, Bezeichnung);
(g) eine Benennung des Personals, welches Proben nimmt;
(h) Informationen zur verwendeten Software oder Hardware zur Probennahme (insofern eingesetzt);
(i) Ggf. die verwendeten statistischen Parameter;
(j) das Ergebnis der Probenentnahme.

§ 5.2.6 Ermittlung bei mehreren Standorten

(1) In Situationen, in denen der Cloud-Anbieter einen Datenverarbeitungsvorgang an mehreren Standorten durchführt, sind solche Standorte in den Ermittlungsplan einzubeziehen (s. IAF MD 5:2015 Tz. 9.1).
(2) Die Zertifizierungsstelle muss über dokumentierte Verfahren verfügen, um Ermittlungen im Rahmen des Multi-Standort-Verfahrens ausführen zu können (s. IAF MD 1:2018 Tz. 7). In diesen Verfahren ist niederzulegen, wie sich die Zertifizierungsstelle davon überzeugt, wie ein Datenverarbeitungsvorgang an allen Standorten durchgeführt wird und dieser auch tatsächlich an allen Standorten die Zertifizierungskriterien erfüllt.
(3) Die durchgeführten Ermittlungsverfahren bei mehreren Standorten sollten jeweils vollständig dokumentiert und im Hinblick auf ihre Wirksamkeit beurteilt werden (darunter Prinzipien und Vorgehensweisen bei der Ermittlung) (s. IAF MD 5:2015 Tz 9.4).
(4) Die Zertifizierungsstelle fordert vom Cloud-Anbieter die Festlegung einer Zentrale (nicht notwendigerweise der Hauptsitz der Organisation), in der zur Erbringung des Datenverarbeitungsvorgangs maßgebliche Prozesse/Tätigkeiten/Systeme geplant, durchgeführt bzw. betrieben und kontrolliert werden (Schlüsseltätigkeiten), sowie bei Bedarf eine Reihe von (permanenten, temporären oder virtuellen) Nebenstandorten, an denen ähnliche oder weitere Prozesse/Tätigkeiten/Systeme vollständig oder teilweise ausgeführt werden (s. IAF MD 1:2018 Tz. 2.4, 5.2, 5.6).
(5) Standorte müssen in die Ermittlung vollständig einbezogen werden, wenn an diesen Schlüsseltätigkeiten des Cloud-Anbieters ausgeübt werden (bspw. Betrieb der Recheninfrastruktur, insofern der Cloud-Anbieter hierfür verantwortlich). Somit muss mindestens die Zentrale zwingend geprüft werden.

(6) Es ist erlaubt Stichproben von Nebenstandorten zu nehmen, insbesondere wenn diese Standorte sehr ähnliche Prozesse/Tätigkeiten ausführen (s. IAF MD 1:2018 Tz. 4.6, 6.1.1.1). Die Festlegung der Stichproben muss im Ergebnis jedoch eine repräsentative Auswahl der unterschiedlichen Standorte gewährleisten und sicherstellen, dass alle im Zertifizierungsumfang enthaltenen Kriterien überprüft werden (s. IAF MD 1:2018 Tz. 6.1.2.1).

(7) Bei der Festlegung des Umfangs der Stichprobe muss die Zertifizierungsstelle folgendes beachten (s. IAF MD 1:2018 Tz. 6.1.3):

(a) Die Zertifizierungsstelle muss über ein dokumentiertes Verfahren zur Bestimmung der Größe der Stichprobe verfügen.
(b) Die Zertifizierungsstelle muss jedes durchgeführte Stichprobenverfahren dokumentieren.
(c) Die Mindestanzahl an Standorten, die pro Ermittlung zu begehen sind, ist:
    (i) Erstprüfung: der Umfang der Stichprobe muss die Quadratwurzel der Anzahl der Nebenstandorte sein: ($y=\sqrt{x}$), gerundet auf die höhere ganze Zahl, wobei y = die Anzahl an Nebenstandorten ist, die in die Stichprobe aufzunehmen sind und x = die Gesamtanzahl an Nebenstandorten.
    (ii) Überwachungsprüfung: der Umfang der jährlichen Stichprobe muss die Quadratwurzel der Anzahl der Standorte sein, multipliziert mit dem Faktor von 0,6 als Koeffizient ($y=0{,}6*\sqrt{x}$), aufgerundet auf die nächste ganze Zahl.
(d) Die Zentrale muss während jeder Erstzertifizierung und mindestens einmal jährlich als Teil der Überwachung überprüft werden.
(e) Mindestens 25 % der Stichproben sind nach dem Zufallsprinzip auszuwählen (s. IAF MD 1:2018 Tz. 6.1.2.2). Der Rest ist so auszuwählen, dass die Unterschiede der Standorte, die über den Gültigkeitszeitraum der Zertifizierung ausgewählt werden, so groß wie möglich sind (s. IAF MD 1:2018 Tz. 6.1.2.3). Zudem muss über den Gültigkeitszeitraum der Zertifizierung jeder Standort mindestens einmal überprüft werden.
(f) Der Umfang oder die Häufigkeit der Stichprobe wird erhöht, wenn die Risikoanalyse der Zertifizierungsstelle für den Datenverarbeitungsvorgang oder den Nebenstandorten besondere Umstände erkennen lässt (bspw. Veränderungen des Standorts, Ergebnisse interner Audits des Cloud-Anbieters, Veränderung von Risiken).
(g) Bei Änderung der Struktur des Cloud-Anbieters (bspw. Aufnahme eines neuen Standorts) passt die Zertifizierungsstelle die Stichprobenverfahren an. Dazu gehört die Erwägung, ob der/die neue(n) Standort(e) zu prüfen ist/sind oder nicht.

Beispiel:
- 1 Hauptniederlassung (Zentrale): Begehung bei jedem Ermittlungszyklus (Erstprüfung und Überwachungsprüfung)
- 4 nationale Zweigstellen: Stichprobe = 2: mindestens 1 nach dem Zufallsprinzip
- 27 regionale Geschäftsstellen: Stichprobe = 6: mindestens 2 nach dem Zufallsprinzip

(8) Zertifizierungsstellen müssen dokumentierte Verfahren haben, um Stichprobenverfahren dort einzuschränken, wo diese nicht angemessen sind, um ausreichend Vertrauen zu schaffen (s. IAF MD 1:2018 Tz. 6.1.1.4, 6.1.2.4, IAF MD 5:2015 Tz. 9.2, 10.3). Solche Einschränkungen können im Hinblick auf folgende Faktoren durch die Zertifizierungsstelle festgelegt sein:

(a) die Risiken für einen Datenverarbeitungsvorgang für einen Standort;
(b) Gesamtanzahl des Personals am Standort;
(c) signifikante Unterschiede in der Größe der Standorte;
(d) Komplexität der Tätigkeiten am Standort;
(e) Abweichungen im Geschäftszweck der Standorte;
(f) Abweichungen in Arbeitsverfahren oder den durchgeführten Aktivitäten;
(g) Komplexität der Informationssysteme an den verschiedenen Standorten;
(h) mögliche Wechselwirkungen mit kritischen Informationssystemen;
(i) Vorhandensein von mehreren/eigenen Datenschutzmanagementsystemen pro Standort;
(j) Variationen des Designs und der Funktionsweise der Steuerungen;
(k) Aufzeichnungen zu Beschwerden und anderen relevanten Aspekten zu Korrektur- und vorbeugenden Maßnahmen;
(l) Vorfälle im Bereich der Daten- und Informationssicherheit an den einzelnen Standorten.
(m) Ergebnisse interner Audits an den Standorten und Managementbewertungen oder frühere Zertifizierungsaudits;
(n) abweichende gesetzliche Anforderungen;
(o) Unterschiede in Kultur oder Sprache;

(p) geografische Standortverteilung;
(q) handelt es sich um permanente oder temporäre Standorte.

(9) Stellt die Zertifizierungsstelle fest, dass kein stichprobenbasiertes Verfahren angewendet werden kann, so ist eine einzelne Prüfung der Standorte erforderlich (s. IAF MD 1:2018 Tz. 1, 4.6, 6.2):

(a) Das Ermittlungsprogramm muss eine Erstprüfung für alle Standorte vorsehen.
(b) Bei Überwachungsprüfungen sind 30 % aller Standorte, gerundet auf die nächste ganze Zahl, jährlich zu prüfen.
(c) Jede Prüfung muss die Zentrale umfassen.
(d) Die für die zweite Überwachungsprüfung ausgewählten Standorte unterscheiden sich in der Regel von denjenigen Standorten, die für die erste Überwachungsprüfung ausgewählt wurden.

(10) Üblicherweise würden an Nebenstandorten Vor-Ort-Prüfungen durchgeführt werden. Jedoch sollten die folgenden Verfahren als mögliche Alternativen berücksichtigt werden, um einige Vor-Ort-Prüfungen zu ersetzen (s. IAF MD 5:2015 Tz. 9.3):

(a) Persönliche Interviews oder Treffen oder Telefonkonferenzen mit dem Cloud-Anbieter;
(b) Überprüfung von Tätigkeiten an Nebenstandorten anhand von Dokumenten;
(c) Fernabfrage von elektronischen Standorten, die Aufzeichnungen oder anderweitige Informationen beinhalten, die in Bezug auf den Datenverarbeitungsvorgang und den/die Nebenstandort(e) begutachtungsrelevant sind;
(d) Nutzung von Video- und Telefonkonferenzen sowie anderen Technologien, die eine wirksame Ermittlung aus der Ferne ermöglichen.

§ 5.2.7 Ermittlungsbericht

(1) Die Evaluatoren erstellen auf der Grundlage der Ermittlung einen Ermittlungsbericht, indem die Ermittlungsergebnisse genau, klar, eindeutig und objektiv dargelegt werden (s. ISO/IEC 17065:2012 Tz. 7.4.9, DSK Tz. 7.4).
(2) Im Allgemeinen muss der Ermittlungsbericht die zwei geprüften Ebenen beim Cloud-Anbieter wiederspiegeln. Zum einen das Datenschutz-Managementsystem des Cloud-Anbieters als Organisation und zum anderen die Erfüllung der Zertifizierungskriterien in Bezug auf den zu zertifizierenden Datenverarbeitungsvorgang.
(3) Der Ermittlungsbericht enthält mindestens folgende Angaben:

(a) eindeutige Kennzeichnung, so dass alle Teile des Ermittlungsberichts als Teil eines vollständigen Berichts erkannt werden sowie eine eindeutige Kennzeichnung des Endes;
(b) das Ausstellungsdatum des Berichts;
(c) Angaben zu den Evaluatoren zur Durchführung des Ermittlungsverfahrens, darunter den Namen und die Unternehmensanschrift;
(d) Angaben zum Cloud-Anbieter, darunter den Namen und die Anschrift;
(e) eine detaillierte Beschreibung des Zertifizierungsgegenstandes, mit Angabe aller relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird (s. § 5.1.4);
(f) eine Darstellung des zeitlichen Ablaufs, darunter mindestens das Start- und Enddatum der Ermittlung;
(g) eine Darstellung des Umfangs der Ermittlung mit Angabe der Standorte und Räumlichkeiten, an bzw. in denen die Ermittlung erfolgt ist, einschließlich wenn sie in den Räumlichkeiten des Cloud-Anbieters oder an anderen Orten als den permanenten Räumlichkeiten der Evaluatoren oder Zertifizierungsstelle oder in zugehörigen zeitweiligen oder mobilen Räumlichkeiten durchgeführt werden;
(h) die Maßnahmen, welche die Evaluatoren zur Ermittlung angewendet hat, insbesondere Angaben zu Ermittlungsmethoden nach § 5.2.4 und –sofern für das Verständnis erforderlich– eine Begründung für deren Einsatz;
(i) eine Aufstellung der geprüften Objekte (s. § 5.2.3);
(j) Angaben zur Verwendung technischer Prüfsoftware und -hardware (z.B. verwendete Programme zur Durchführung von technischen Ermittlungen);
(k) die Angabe der durch die Zertifizierungsstelle anerkannten Zertifikate sowie die Ergebnisse über die stichprobenartige Überprüfung;
(l) eine Aussage über die Prüfung des Zusammenwirkens der Datenverarbeitungsvorgänge;

(m) ggf. Angaben über spezielle Ermittlungsbedingungen, wie etwa Umgebungsbedingungen;
(n) bei Bedarf, welche Ermittlungsungenauigkeiten auftreten können, oder welche Gefahren für Ermittlungsgenauigkeit, -wiederholbarkeit und -reproduzierbarkeit bestehen (s. ISO/IEC 17007 Tz. 5.4.1);
(o) eine Beschreibung der Umsetzung des Datenschutz-Managementsystemeine Beschreibung der Umsetzung der einzelnen Zertifizierungskriterien. Hierbei ist der Detailgrad der Beschreibung mindestens so umfassend zu wählen, dass alle notwendigen Informationen enthalten sind, um eine eindeutige Bewertung der Konformität zu einzelnen Zertifizierungskriterien zweifelsfrei und ohne Unsicherheiten durchführen zu können;
(p) wenn erforderlich, eine Aussage zur Konformität mit den einzelnen Zertifizierungskriterien. Die Evaluatoren müssen bezüglich der Aussage zur Konformität so berichten, dass deutlich wird, für welche Ergebnisse die Aussage zur Konformität gilt, welche Zertifizierungskriterien von einem Ermittlungsobjekt erfüllt oder nicht erfüllt werden, und welche Entscheidungsregel angewendet wurde. Meinungen und Interpretationen von Aussagen aus Ermittlungen sind von Aussagen zur Konformität erkennbar abzugrenzen;
(q) die Erklärung eines Evaluators, dass er die Zertifizierungsanforderungen dieses Konformitätsbewertungsprogramms bezüglich Unabhängigkeit und Unparteilichkeit erfüllt hat und keine Befangenheit vorliegt.

(4) Der Ermittlungsbericht ist im Akkreditierungsverfahren und jederzeit auf Wunsch der Datenschutzaufsichtsbehörde vollumfänglich zugänglich zu machen (s. EDPB Annex 1 Tz. 7.4).
(5) Die Evaluatoren müssen für alle im Bericht bereitgestellten Informationen die Verantwortung tragen, es sei denn, die Informationen werden vom Cloud-Anbieter oder einer dritten Partei bereitgestellt. Daten, die von einem Cloud-Anbieter oder einer dritten Partei bereitgestellt werden, müssen eindeutig gekennzeichnet werden. Zusätzlich muss der Bericht eine Aussage enthalten, wenn die Informationen vom Cloud-Anbieter oder einer dritten Partei bereitgestellt werden und sich auf die Validität der Ermittlungsergebnisse auswirken können.
(6) Die Evaluatoren stellen den Ermittlungsbericht elektronisch oder als Papierversion der Zertifizierungsstelle und dem Cloud-Anbieter zur Verfügung und räumen diesen uneingeschränkte Nutzungsrechte ein. Der Cloud-Anbieter darf den Ermittlungsbericht Dritten nur im vollen Wortlaut und unter Angabe des Ausstellungsdatums zur Verfügung stellen und hat solchen Dritten entsprechende Nutzungsbeschränkungen aufzuerlegen. Die Zertifizierungsstelle kann sich das Recht zur Veröffentlichung und zur öffentlichen Wiedergabe i.S.d. § 15 Abs. 2 UrhG vorbehalten.
(7) Wenn ein ausgestellter Bericht geändert oder neu ausgestellt werden muss, müssen alle Änderungen von Informationen eindeutig gekennzeichnet werden und, wo erforderlich, muss der Grund für die Änderung im Bericht aufgenommen werden. Änderungen an einem Bericht nach der Ausstellung dürfen nur in Form eines gesonderten Schriftstücks oder einer Datenübertragung erfolgen, worin der Hinweis „Ergänzung zu Bericht, Dokumenten-ID ... [oder sonstige Kennzeichnung]“ oder ein gleichwertiger Wortlaut enthalten ist. Wenn es erforderlich ist, einen vollständigen neuen Bericht auszustellen, muss dieser Bericht eine eindeutige Bezeichnung haben und einen Verweis auf das Original enthalten, welches er ersetzt.

5.3 Bewertung

§ 5.3.1 Bewertung der Ermittlungsergebnisse

(1) Die Entscheider erstellen auf der Grundlage der Evaluierung eine Bewertung der Erfüllung der Zertifizierungskriterien des AUDITOR-Kriterienkatalogs durch die Datenverarbeitungsvorgänge in Bezug auf eine bestimmte Schutzklasse. Dabei ist sowohl eine Bewertung hinsichtlich der Erfüllung der einzelnen Zertifizierungskriterien des AUDITOR-Kriterienkatalogs als auch hinsichtlich der Erfüllung der gesamten Zertifizierungskriterien des AUDITOR-Kriterienkatalogs, jeweils bezogen auf eine bestimmte Schutzklasse, erforderlich.
(2) Die Bewertung wird durch Personal der Zertifizierungsstelle (Entscheider) vorgenommen, welches nicht an Ermittlungstätigkeiten beteiligt war, um möglichen Interessenkonflikten vorzubeugen und Unparteilichkeit sicherzustellen (s. ISO/IEC 17065:2012 Tz. 7.5.1, DSK Tz. 7.5). Die Zertifizierungsstelle hat darzulegen, wie die mit der Bewertung beauftragte(n) Person(en) weder direkt noch indirekt in den Ermittlungsprozess involviert war(en). Die Umsetzung dieser Anforderungen und deren Ergebnisse sind im Rahmen der Bewertung zu dokumentieren (s. DSK Tz. 7.5).

(3) Empfehlungen für eine Zertifizierungsentscheidung, die sich auf die Bewertung stützt, müssen dokumentiert werden, sofern Bewertung und Zertifizierungsentscheidung nicht gleichzeitig durch dieselbe Person erfolgen (s. ISO/IEC 17065:2012 Tz. 7.5.2). Die Zertifizierungsstelle muss derart berichten, dass deutlich wird, für welche Ergebnisse die Aussage zur Konformität gilt, welche Zertifizierungskriterien von einem Zertifizierungsgegenstand erfüllt oder nicht erfüllt werden, und welche Entscheidungsregel angewendet wurde.
(4) Die Zertifizierungsstelle kann zusätzliche Auskünfte und Nachweise vom Cloud-Anbieter erheben, soweit dies für die Bewertung erforderlich ist.
(5) Soweit einzelne Zertifizierungskriterien des AUDITOR-Kriterienkatalogs für den jeweiligen Zertifizierungsgegenstand nicht anwendbar sind (s. § 5.1.5), ist dies im Rahmen der Begründung des Gesamtergebnisses gesondert aufzuführen und zu begründen.
(6) Die Bewertung mündet in eine Empfehlung für die Entscheidung über die Zertifizierung.

§ 5.3.2 Nichtkonformitäten von Zertifizierungskriterien

(1) Der Entscheider nimmt eine Bewertung der Konformität von Zertifizierungskriterien vor. Dafür muss die Konformität jeder einzelnen Nummer pro Zertifizierungskriterium bewertet werden. Hierbei soll der folgende Bewertungsmaßstab pro Nummer für ein Zertifizierungskriterium angewandt werden:

- (a) Erfüllung
  - (i) Nummer vom Zertifizierungskriterium ist erfüllt.
- (b) Erfüllung mit Empfehlung
  - (i) Abweichung, die in ihrer Geringfügigkeit die Einhaltung der Datenschutzanforderungen insgesamt nicht in Frage stellt (Verbesserungspotential).
  - (ii) Beispiele:
    1. Das eingesetzte Verschlüsselungsverfahren ist gerade noch „Stand der Technik“, sollte aber zeitnah ausgetauscht werden.
    2. Da keine Passwortrichtlinie bzgl. der erneuten Verwendung von Passwörtern gesetzt ist, können Mitarbeiter ein ursprüngliches Passwort erneut verwenden.
    3. Das IT-Sicherheitshandbuch sollte gepflegt werden und einer standardisierten Methodik folgen.
- (c) Nichtkonformität
  - (i) Wesentliche Abweichung sodass erheblicher Zweifel besteht, dass die Datenschutzanforderungen grundsätzlich eingehalten werden.
  - (ii) Beispiele:
    1. Die benötigten Dokumentationen (z.B. Prozessdokumentation, Funktionsdokumentation oder Logs) können nicht vom Cloud-Anbieter vorgelegt werden oder die Durchführung von Datenverarbeitungsvorgängen zur Überprüfung der Einhaltung von Kriterien ist nicht möglich.
    2. Prozessdokumentationen liegt vor, diese wird jedoch beim Cloud-Dienst-Betrieb nicht fortlaufend durchgeführt (‚gelebt‘).
    3. Sicherheitstests haben schwerwiegende Mängel oder Schwachstellen in der eingesetzten Software des Cloud-Dienstes ergeben.
    4. Befragung oder Vor-Ort-Prüfung im Rahmen eines Audits hat die fehlende Umsetzung von Zertifizierungskriterien aufgedeckt.

(2) Wird eine Nummer eines Kriteriums mit „Nichtkonformität“ bewertet, so gilt dieses Kriterium auch als nicht erfüllt.
(3) Nichtkonformitäten müssen vor Erteilung einer Zertifizierung behoben sein.
(4) Wurde bei der Bewertung festgestellt, dass eine oder mehrere Zertifizierungskriterien nicht erfüllt sind, prüft die Zertifizierungsstelle, ob eine Nachbesserung in angemessener Frist vom Cloud-Anbieter erfolgreich durchgeführt werden kann (s. ISO/IEC 17065:2012 Tz. 7.4.7). Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.
(5) Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, welche Mängel oder Abweichungen vorliegen, die eine Erfüllung der Zertifizierungskriterien verhindern (s. ISO/IEC 17065:2012 Tz. 7.4.6, EDPB Annex 1 Tz. 7.4). Die Zertifizierungsstelle muss bei etwaigen Rückfragen zur Klärung von Unklarheiten beitragen, soweit die Unparteilichkeit dadurch nicht gefährdet wird.
(6) Die Zertifizierungsstelle muss vom Cloud-Anbieter fordern, die Ursachen zu analysieren und die spezifischen, durchgeführten oder geplanten Korrekturen und Korrekturmaßnahmen zu

beschreiben, um die erkannten Nichtkonformitäten in einem festgelegten Zeitraum zu beseitigen.

(7) Im Rahmen der Nachbesserung muss der Cloud-Anbieter dafür Sorge tragen, dass alle Mängel und Abweichungen zur Erfüllung der Zertifizierungskriterien abgestellt werden.

(8) Der Cloud-Anbieter stellt der Zertifizierungsstelle nach Abschluss der Nachbesserung alle notwendigen Dokumente zur Verfügung, um die erfolgreiche Nachbesserung belegen zu können.

(9) Die Zertifizierungsstelle muss die vom Cloud-Anbieter vorgelegten Korrekturen und Korrekturmaßnahmen bewerten, um festzustellen, ob sie annehmbar sind (s. ISO/IEC 17065:2012 Tz. 7.4.7, 7.4.8). Die Zertifizierungsstelle muss die Wirksamkeit aller durchgeführten Korrekturen und Korrekturmaßnahmen verifizieren. Die erlangten Nachweise über die Behebung der Nichtkonformitäten müssen aufgezeichnet werden. Der Cloud-Anbieter muss über das Ergebnis der Überprüfung und Verifizierung informiert werden.

(10) Die Zertifizierungsstelle kann abhängig von dem Umfang und der Schwere der erforderlichen Nachbesserung eine Nachprüfung mit angemessener Frist zur Durchführung ansetzen. Im Rahmen dieser Nachprüfung gelten die Zertifizierungsanforderungen der Ermittlung und es sind entsprechende Ermittlungstätigkeiten nach § 5.2.4 ggf. stichprobenartig anzuwenden.

(11) Wurde bei der Bewertung der Korrekturen oder der Nachprüfung festgestellt, dass eine oder mehrere Zertifizierungskriterien weiterhin nicht erfüllt sind, prüft die Zertifizierungsstelle, ob eine weitere Nachbesserung in angemessener Frist vom Cloud-Anbieter erfolgreich durchgeführt werden kann und angemessen erscheint. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.

(12) Im Rahmen der Überwachung wird von der Zertifizierungsstelle geprüft, ob den Empfehlungen entsprochen wurde. Wenn nicht, prüft die Zertifizierungsstelle, ob die bisherige Empfehlung aufgrund geänderter Rahmenbedingungen zur Nichtkonformität geworden ist.

§ 5.3.3 Nichtkonformitäten von Zertifizierungskriterien an verschiedenen Standorten

(1) Wenn Nichtkonformitäten an einzelnen Standorten gefunden werden, entweder während des internen Audits des Cloud-Anbieters oder während der Ermittlung durch die Zertifizierungsstelle, muss ermittelt werden, ob die anderen Standorte ebenfalls betroffen sein können (s. IAF MD 1:2018 Tz. 7.7.1). Aus diesem Grund muss die Zertifizierungsstelle von dem Cloud-Anbieter fordern, dass diese ihre Nichtkonformitäten überprüft, um festzustellen, ob diese ein allgemeines Defizit des Cloud-Dienstes, welches auch auf andere Standorte zutrifft, darstellen oder nicht.

(2) Falls festgestellt wird, dass dies der Fall ist, so müssen Korrekturmaßnahmen durchgeführt und geprüft werden, und zwar sowohl in der Zentrale, als auch an den einzelnen betroffenen Nebenstandorten (s. IAF MD 1:2018 Tz. 7.7.1).

(3) Falls festgestellt wird, dass dies nicht der Fall ist, muss der Cloud-Anbieter in der Lage sein, gegenüber der Zertifizierungsstelle nachzuweisen, dass eine Einschränkung der Folgemaßnahmen gerechtfertigt ist (s. IAF MD 1:2018 Tz. 7.7.1).

(4) Falls zum Zeitpunkt des Entscheidungsprozesses einer der Standorte eine Nichtkonformität aufweist, muss die Zertifizierung gegenüber der gesamten Multi-Standort-Organisation verweigert werden, bis zufriedenstellende Korrekturmaßnahmen umgesetzt wurden (s. IAF MD 1:2018 Tz. 7.7.3, 7.7.4). Es ist nicht erlaubt, dass der Cloud-Anbieter einen „problematischen" Standort während des Zertifizierungsprozesses ausschließt, um die Hindernisse, die durch die Existenz einer Nichtkonformität bei einem einzelnen Standort aufgetreten sind, zu überwinden.

5.4 Entscheidung über die Zertifizierung

§ 5.4.1 Entscheidung der Zertifizierungsstelle

(1) Die Entscheider entscheiden auf Grundlage des Ermittlungsberichts und der Bewertung über die Erteilung der Zertifizierung und die Verleihung der Konformitätszeichen.

(2) Der Zeitraum zwischen dem Abschluss der letzten Ermittlung und der Zertifizierungsentscheidung darf nur in berechtigten Ausnahmefällen die Dauer von 3 Monaten überschreiten (s. DSK Tz. 7.3).

(3) Die Zertifizierungsentscheidung darf nur von durch die Zertifizierungsstelle benannten Personen (Entscheider) getroffen werden, die über einen Vertrag oder eine formale Vereinbarung gebunden sind an (s. ISO/IEC 17065:2012 Tz.7.6.3 und 7.6.4):

(a) die Zertifizierungsstelle;
(b) eine Einheit unter Organisationskontrolle der Zertifizierungsstelle.

(4) Die Zertifizierungsentscheidung muss von einer Person oder Gruppe von Personen (z. B. ein Komitee), die nicht an den Ermittlungstätigkeiten beteiligt waren, durchgeführt werden (s. ISO/IEC 17065:2012 Tz. 7.6.2). Die Bewertung und Entscheidung über die Zertifizierung können gleichzeitig durch dieselbe Person oder Personengruppe durchgeführt werden.
(5) Die Entscheidung über die Zertifizierung muss durch den Leiter der Zertifizierungsstelle oder eine direkt von ihm beauftragte qualifizierte Person erfolgen (s. DSK Tz. 7.6).
(6) Die Zertifizierungsstelle muss detailliert darlegen, wie ihre Unabhängigkeit und Verantwortlichkeit im Hinblick auf die Zertifizierungsentscheidungen sichergestellt werden (s. DSK Tz. 7.6, EDPB Annex 1 Tz. 7.6).
(7) Die Zertifizierungsstelle muss den Cloud-Anbieter über eine Entscheidung, die Zertifizierung nicht zu gewähren, unter Nennung der Gründe informieren (s. ISO/IEC 17065:2012 Tz. 7.6.6). Wenn der Cloud-Anbieter Interesse an der Fortsetzung des Zertifizierungsprozesses äußert, kann die Zertifizierungsstelle die Auswahl- und Ermittlungsprozesse wiederaufnehmen.

§ 5.4.2 Einspruch durch den Cloud-Anbieter

(1) Der Cloud-Anbieter kann gegen eine Entscheidung Einspruch bei der Zertifizierungsstelle einlegen. Der Einspruch ist zu begründen.
(2) Ein Einspruch ist ein Verlangen des Cloud-Anbieters gegenüber einer Zertifizierungsstelle, ihre Entscheidung bezüglich des Zertifizierungsgegenstands zu überprüfen (s. ISO/IEC 17000:2004 Tz. 6.4).
(3) Der Einspruch ist in Textform innerhalb einer Frist von 4 Wochen nach Zugang der Zertifizierungsentscheidung einzureichen.
(4) Die Zertifizierungsstelle prüft, ob der Einspruch begründet ist.
(5) Soweit sich der Einspruch gegen die Auswahl- oder Ermittlungstätigkeiten oder die Feststellungen der Evaluatoren richtet, informiert die Zertifizierungsstelle die Evaluatoren über den Einspruch und holt eine Stellungnahme der Evaluatoren ein.
(6) Soweit der Einspruch gerechtfertigt ist, ändert die Zertifizierungsstelle die Zertifizierungsentscheidung. Soweit die Zertifizierungsstelle dem Einspruch nicht abhilft, ist dies zu begründen.
(7) Die Entscheidung über den Einspruch einschließlich Begründung ist dem Cloud-Anbieter in Textform mitzuteilen.

5.5 Bestätigung

§ 5.5.1 Erteilung der Zertifizierung

(1) Die Zertifizierung ist durch die Zertifizierungsstelle im beantragten Umfang zu erteilen, wenn die Datenverarbeitungsvorgänge die Zertifizierungskriterien des AUDITOR-Kriterienkatalogs erfüllen und die Zertifizierungsstelle die zuständige Datenschutz-Aufsichtsbehörde über die Gründe für die Erteilung der Zertifizierung informiert hat.
(2) Die Zertifizierungsstelle unterrichtet die zuständige Datenschutz-Aufsichtsbehörde über die Zertifizierung schriftlich mindestens eine Woche vor Erteilung der Zertifizierung (s. DSK Tz. 7.6, EDPB Annex 1 Tz. 7.8). Diese Unterrichtung muss den Namen der Zertifizierungsstelle, die Beschreibung des Zertifizierungsgegenstands und das öffentliche Kurzgutachten enthalten.

§ 5.5.2 Erteilen des Rechts zur Nutzung von Konformitätszeichen

(1) Die Erteilung der Zertifizierung berechtigt den Cloud-Anbieter für die zertifizierten Datenverarbeitungsvorgänge ein Gütesiegel und ein Zertifikat als entsprechende Konformitätszeichen zu führen.
(2) Die Zertifizierungsstelle vergibt für jede Zertifizierung eine eindeutige Zertifizierungsnummer. Sie setzt sich zusammen aus der eindeutigen Bezeichnung der Zertifizierungsstelle, der Angabe „AUDITOR“ und einer innerhalb der Zertifizierungsstelle eindeutigen Nummer (Beispiel: ZERTIFIZIERUNGSSTELLE-AUDITOR-0001). Die Zertifizierungsnummer ist auf allen Konformitätszeichen zur Rückverfolgbarkeit anzugeben.
(3) Ein Konformitätszeichen darf nur während der Gültigkeit der Zertifizierung und der Akkreditierung der Zertifizierungsstelle geführt werden.
(4) Die Zertifizierungsstelle stellt die Konformitätszeichen aus:

   (a) Das Zertifikat wird dem Cloud-Anbieter postalisch und elektronisch zur Verfügung gestellt.
   (b) Das Gütesiegel wird graphisch in elektronischer Form zur Verfügung gestellt.

(5) Die Zertifizierungsstelle stellt die korrekte Verwendung des Konformitätszeichens für die Gültigkeitsdauert sicher (s. § 4.4.3).

§ 5.5.3 Inhalt des Gütesiegels

(1) Das Gütesiegel enthält folgende Angaben:

(a) das graphische Konformitätszeichen;
(b) Kurztitel Datenverarbeitungsvorgang und Rolle Datenschutzrolle („als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO“);
(c) die Zertifizierungsnummer;
(d) die Gültigkeitsdauer der Zertifizierung mit Angabe des Zeitraums (Ausstellung, Laufzeit bis);
(e) die Bezeichnung AUDITOR mit Schutzklasse 1, 2 oder 3;
(f) die Angabe des Wiederherstellbarkeitsklasse 1, 2 oder 3.

(2) Wird das Gütesiegel in elektronischen Medien (bspw. Webseite) angebracht, so ist dieses mit einem Link auf den Eintrag im Zertifizierungsregister der Zertifizierungsstelle zu versehen (s. § 4.4.2), um die Rückverfolgbarkeit durch Cloud-Nutzer und Interessierte Parteien zu ermöglichen.

§ 5.5.4 Inhalt des Zertifikats

(1) Das Zertifikat enthält folgende Angaben:

(a) den Cloud-Anbieter, ggf. als Kurzbezeichnung;
(b) Anschrift des Cloud-Anbieters, ggf. Nebenstandorte;
(c) Datenschutzrolle gemäß DSGVO „als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO“;
(d) Geltungsbereich Regional: Deutschland, EU, Drittland;
(e) den Zertifizierungsgegenstand, ggf. als Kurzbezeichnung;
(f) die Zertifizierungsstelle und deren Anschrift;
(g) die Zertifizierungsaussage, wonach die zertifizierten Datenverarbeitungsvorgänge die einschlägigen Vorgaben der DSGVO und des BDSGs gemäß dem AUDITOR-Kriterienkatalog in der jeweiligen Fassung für eine konkrete Schutzklasse und eine konkrete Wiederherstellbarkeitsklasse sowie die zusätzlichen Anforderungen der Datenschutzaufsichtsbehörden erfüllt;
(h) die Bezeichnung der maßgeblichen Fassung des AUDITOR- Konformitätsbewertungsprogramm und des -Kriterienkatalogs;
(i) eine eindeutige Zertifizierungsnummer;
(j) Tag der Zertifizierungsentscheidung;
(k) Angabe letzter Audittag vor Ort: <tt.mm.jjjj> /Berichtsnummer/Datum;
(l) die Gültigkeitsdauer der Zertifizierung mit Angabe des Zeitraums, Datum der Ausstellung des Zertifikats: „Datum der Ausstellung <tt.mm.jjjj>“ und „Laufzeit bis <tt.mm.jjjj> max. 3 Jahre>“;
(m) Kurzangabe zur Überwachung, bspw. „innerhalb der Laufzeit des Zertifikats jährlich auf Konformität überwacht wird“; und „nächste geplante Überwachung bis spätestens <tt.mm.jjjj>“
(n) Angabe zur Mitteilung der Entscheidung an die Datenschutzaufsichtsbehörde „Die Gründe für die Erteilung des Zertifikats wurden der [Datenschutzaufsichtsbehörde XYZ] gemäß Art. 43 Abs. 5 DSGVO am TT.MM.JJJJ mitgeteilt.“
(o) eine Anlage mit den Angaben nach (2); sowie die Hinweise auf diese Anlagen „[Datenverarbeitungsvorgang] gemäß Anlage 1“ und „unter Beachtung der Nutzungsausschlüsse gemäß Anlage 2“.
(p) Akkreditierungssymbol;
(q) Ggf. Logo der Zertifizierungsstelle;
(r) Unterschrift Leitung der Zertifizierungsstelle oder Vertreter.

(2) Die Anlage zum Zertifikat enthält folgende Angaben:

(a) Anlage 1:
    (i) die eindeutige Bezeichnung des Cloud-Anbieters, inkl. Anschrift;
    (ii) die ausführliche Beschreibung des Zertifizierungsgegenstands;
    (iii) Verweis auf das öffentliche Kurzgutachten über das Ergebnis der Zertifizierung gem. Tz. 7.6 und 7.8 der Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065 der Datenschutzkonferenz (DSK). Das Kurzgutachten muss die Nutzung des Zertifzierungsgegenstands im Einsatzgebiet und im Anwendungsfall in transparenter und nachvollziehbarer

Weise dokumentieren, so dass auch der (End-) Kunde bzw. eine betroffene Person in angemessener Zeit nachvollziehen kann, was unter Nutzung des Zertifizierungsgegenstands im datenschutzrechtlichen Sinn gewährleistet ist;
(iv) ggf. die Bezeichnung der angewendeten Regelwerke der Zertifizierungsstelle;
(v) ggf. weitere Hinweise der Zertifizierungsstelle.

(b) Anlage 2:
(i) Darin sind alle Nutzungsausschlüsse zu nennen, d.h. was unter Einsatz des Zertifizierungsgegenstands im Anwendungsgebiet nicht gewährleistet wird.

(3) Ferner sei auf das *„Merkblatt zu Akkreditierungsverfahren im Datenschutz“* hingewiesen, welches im Anhang ein Musterzertifikat aufweist.

§ 5.5.5 Gültigkeitsdauer und Aufrechterhalten der Zertifizierung

(1) Die Zertifizierung wird für eine Gültigkeitsdauer von drei Jahren erteilt. Die Frist beginnt mit dem im Konformitätszeichen ausgewiesenen Datum der Erteilung.
(2) Der Cloud-Anbieter kann vor oder nach Ablauf der Gültigkeitsdauer die Aufrechterhaltung der Zertifizierung in Form einer Verlängerung der Zertifizierung beantragen. In diesem Fall wird der Zertifizierungsgegenstand erneut geprüft und zertifiziert.
(3) Die Zertifizierungsstelle kann die erneute Zertifizierung bei rechtzeitiger Beantragung und abgeschlossenem Zertifizierungsverfahren auf das Datum unmittelbar nach Ablauf der Gültigkeitsdauer der vorangegangenen Zertifizierung ausstellen.
(4) Werden bestehende Zertifizierungen des Cloud-Anbieters anerkannt, so wird die Gültigkeitsdauer der AUDITOR-Zertifizierung auf das Ablaufdatum der kürzest laufenden und anerkannten Zertifizierung reduziert (s. DSK Tz. 7.4). Bei der Rezertifizierung der anerkannten Zertifizierung wird die Ablauffrist der AUDITOR-Zertifizierung auf die Laufzeit des anerkannten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit der AUDITOR-Zertifizierung von 3 Jahren oder bei weiteren anerkannten Fremdzertifikaten auf die kürzeste Laufzeit. Wird keine Rezertifizierung des anerkannten Zertifikats durchgeführt, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der AUDITOR-Zertifizierung aufrecht zu erhalten.

§ 5.5.6 Einspruch durch die Datenschutzaufsichtsbehörde

(1) Wird die Zertifizierungsstelle von der Datenschutzaufsichtsbehörde angewiesen, eine erteilte Zertifizierung gemäß Art. 58 Abs. 2 lit. h DSGVO zu widerrufen oder keine Zertifizierung zu erteilen, so muss die Zertifizierungsstelle im Rahmen ihres Managementsystems sicherstellen, dass der entsprechende Cloud-Anbieter hierüber und über die Folgen daraus informiert wird, entsprechende Registereinträge angepasst werden und die Datenschutzaufsichtsbehörde hierüber in Kenntnis gesetzt wird (s. DSK Tz. 8.12).

§ 5.5.7 Zertifizierungsdokumentation

(1) Die Zertifizierungsstelle muss dem Cloud-Anbieter eine formelle Zertifizierungsdokumentation bereitstellen, welche die Identifizierung folgender Elemente deutlich vermittelt oder zulässt (s. ISO/IEC 17065:2012 Tz. 7.7.1, EDPB Annex 1 Tz. 7.7):

(a) den Namen und die Anschrift der Zertifizierungsstelle;
(b) das Datum, an dem die Zertifizierung gewährt wurde (das Datum darf nicht vor dem Zeitpunkt liegen, an dem die Entscheidung über die Zertifizierung getroffen wurde);
(c) den Namen und die Anschrift des Cloud-Anbieters;
(d) den Geltungsbereich der Zertifizierung, inkl. einer genauen Abgrenzung der Datenverarbeitungsvorgänge als Zertifizierungsgegenstand;
(e) den Zeitraum oder das Ablaufdatum der Zertifizierung, wenn die Zertifizierung nach einem festgelegten Zeitpunkt abläuft;
(f) die Frequenz und weitere Informationen über notwendige Überwachungstätigkeiten:
(g) Informationen zum Antrag und zu Ermittlungs- und Bewertungsberichten;
(h) Zertifizierungsvereinbarung;
(i) die begründete Bewertung hinsichtlich der Erfüllung, Empfehlung, Nichtkonformität oder Nichtanwendbarkeit der einzelnen Zertifizierungskriterien für die betreffende Schutzklasse;
(j) das Gesamtergebnis hinsichtlich der Erfüllung oder Nichterfüllung der Zertifizierungskriterien für eine bestimmte Schutzklasse;
(k) die Begründung des Gesamtergebnisses;

(l) Ggf. Verifizierung der Korrekturen und Korrekturmaßnahmen;
(m) Ggf. Aufzeichnungen zu Beschwerden und Einsprüchen sowie zu nachfolgenden Korrekturen oder Korrekturmaßnahmen.

(2) Die formelle Zertifizierungsdokumentation muss die Signatur oder eine andere festgelegte Befugnis der Person(en) der Zertifizierungsstelle einschließen, der/denen eine solche Verantwortung zugewiesen wird (s. ISO/IEC 17065:2012 Tz. 7.7.2).
(3) Die Zertifizierungsstelle muss die Aufzeichnungen zu den Antragstellern und Cloud-Anbietern sicher aufbewahren, um sicherzustellen, dass die Information vertraulich bleibt (s. EDPB Annex 1 Tz. 7.12). Aufzeichnungen müssen in einer Weise transportiert, übersendet oder übertragen werden, die die Aufrechterhaltung der Vertraulichkeit sicherstellt. Aufzeichnungen von zertifizierten Cloud-Anbietern und früheren zertifizierten Cloud-Anbietern müssen für die Dauer des laufenden Zyklus zuzüglich eines weiteren, vollständigen Zertifizierungszyklus aufbewahrt werden.
(4) Die Zertifizierungsstelle muss gemäß der ISO/IEC 17065:2012 Tz. 7.8 ein öffentliches Kurzgutachten über das Ergebnis der Zertifizierung veröffentlichen (s. DSK Tz. 7.6, EDPB Annex 1 Tz. 7.8). Darin müssen auch der Zertifizierungsgegenstand (inkl. der Version oder des Funktionszustands), die zugrundeliegenden Kriterien und die angewendeten Ermittlungsmethoden sowie die Ergebnisse ersichtlich sein.

5.6 Überwachung

§ 5.6.1 Durchführung von regelmäßigen Überwachungstätigkeiten

(1) Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Zertifizierung der Überwachung in Form einer mindestens jährlich durchzuführenden Zwischenprüfung.
(2) Darüber hinaus können anlassbezogene Überwachungen bei Auffälligkeiten erfolgen, die eine Nichtkonformität der Zertifizierungskriterien befürchten lassen.
(3) Das Verfahren und die notwendigen Einträge zur Überwachung in der Zertifizierungsvereinbarung mit dem Cloud-Anbieter sind im Akkreditierungsverfahren und auf Wunsch der Datenschutz-Aufsichtsbehörde jederzeit nachzuweisen.
(4) Aufgrund der Zwischenprüfung hat die Zertifizierungsstelle festzustellen, ob die zertifizierten Datenverarbeitungsvorgänge die Zertifizierungskriterien nach der festgelegten Schutzklasse weiterhin erfüllen.
(5) Die Zertifizierungsstelle erinnert den Cloud-Anbieter und bei Bedarf (ausgegliederte) Evaluatoren rechtzeitig an eine anstehende Zwischenprüfung und weist auf die Folge des Unterbleibens der Zwischenprüfung hin.
(6) Die jährliche Zwischenprüfung ist frühestens nach Ablauf des sechsten und spätestens bis zum Ablauf des zwölften Monats ab Zertifizierungserteilung oder der entsprechenden Zeitpunkte der Folgejahre durchzuführen.
(7) Erfolgt die Zwischenprüfung nicht in der festgelegten Frist, ergreift die Zertifizierungsstelle Maßnahmen gemäß § 5.6.4.
(8) Der Cloud-Anbieter ist zur Mitwirkung an Überwachungstätigkeiten zu verpflichten.
(9) Für die Zwischenprüfung gelten die Anforderungen dieses Programms für durchzuführende Auswahl-, Ermittlungs-, Bewertungs-, und Entscheidungstätigkeiten entsprechend (s. ISO/IEC 17065:2012 Tz. 7.9.2).

§ 5.6.2 Umfang der Überwachungstätigkeiten

(1) Der Umfang der Zwischenprüfung ist so zu wählen, dass mindestens die seit der letzten Prüfung erfolgten Änderungen der Datenverarbeitungsvorgänge durch Ermittlungsmethoden (s. § 5.2.4) geprüft werden. Durch geeignete Stichproben (s. § 5.2.5) unter Anwendung der Ermittlungsmethoden ist festzustellen, ob die Datenverarbeitungsvorgänge insgesamt die Zertifizierungskriterien weiterhin erfüllen (s. ISO/IEC 17000:2004 Tz. A.5.4).
(2) Im Rahmen der Überwachung prüft die Zertifizierungsstelle insbesondere, ob anerkannte Zertifikate weiterhin gültig sind. Stellt eine Zertifizierungsstelle fest, dass ein anerkanntes Zertifikat nicht mehr gültig ist und der Cloud-Anbieter die Zertifizierungsstelle auch nicht vorab informiert hat und gemeinsam entsprechende Maßnahmen durchgeführt wurden (bspw. Änderungszertifizierung), ergreift die Zertifizierungsstelle geeignete Maßnahmen gemäß § 5.6.4.
(3) Die jährlich für Überwachungen aufgewendete Gesamtzeit sollte etwa ein Drittel der Ermittlungszeit betragen, die für die Erstzertifizierungsprüfung aufgewendet wurde (s. IAF MD 5:2015 Tz. 5). Die geplante Überwachungszeit sollte von Zeit zu Zeit überprüft werden, um Änderungen zu berücksichtigen, die sich auf die Überwachungszeit auswirken.

(4) Eine kontinuierliche Überprüfung kann durchgeführt werden, um die Einhaltung der Zertifizierungskriterien dauerhaft zu prüfen (s. Lins et al. (2016)). Zur kontinuierlichen Überprüfung können unter anderem test- und monitoring-basierte Prüfverfahren zum Einsatz kommen, welche Daten erheben, die eine Konformität zu den Zertifizierungskriterien nachweisen können (s. Lins et al. (2019)). Die Prüffrequenz ist hierbei abhängig von dem jeweilig zu prüfenden Zertifizierungskriterium.

§ 5.6.3 Bewertung der Überwachungstätigkeiten

(1) Die Evaluatoren erstellen einen Zwischenprüfbericht und übermitteln diesen rechtzeitig vor Ablauf des Zwischenprüfungszeitraums der Zertifizierungsstelle.
(2) Die Zertifizierungsstelle bewertet den Ermittlungsbericht und entscheidet auf der Grundlage des Zwischenprüfbericht der Evaluatoren, der Bewertung und, soweit erforderlich, weiterer Feststellungen unverzüglich über die Aufrechterhaltung, Einschränkung, Aussetzung oder den Widerruf der Zertifizierung (s. § 5.6.4)
(3) Wenn eine Nichtkonformität mit Zertifizierungskriterien, entweder als Ergebnis der Überwachung oder anderweitig, nachgewiesen wird, muss die Zertifizierungsstelle gemäß § 5.6.4 geeignete Maßnahmen in Betracht ziehen und über diese entscheiden (s. ISO/IEC 17065:2012 Tz. 7.11.1).

§ 5.6.4 Feststellung der Nichtkonformität von Zertifizierungskriterien

(1) Der Cloud-Anbieter ist verpflichtet, die Zertifizierungsstelle unverzüglich detailliert zu informieren, wenn ihm bekannt wird, dass die Voraussetzungen für die Erteilung der Zertifizierung nicht vorlagen oder nicht mehr vorliegen (bspw. Erlöschung anerkannte Zertifikate).
(2) Wenn die Zertifizierungsstelle aufgrund der Überwachungstätigkeiten, von Mitteilungen des Cloud-Anbieters oder eines Dritten oder aufgrund sonstiger Umstände Grund zur Annahme hat, dass die Voraussetzungen für die Zertifizierungserteilung nicht vorlagen oder nicht mehr vorliegen (s. auch § 5.3.2 und § 5.3.3), ergreift sie unverzüglich die erforderlichen Maßnahmen, um das Vorliegen der Voraussetzungen festzustellen (s. ISO/IEC 17065:2012 Tz.7.11.1). Darüber hinaus kann die Zertifizierungsstelle folgende Maßnahmen ergreifen:

    (a) die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist;
    (b) die Zertifizierungsstelle kann dem Cloud-Anbieter eine Änderungszertifizierung empfehlen (s. § 5.6.9);
    (c) die Zertifizierungsstelle kann die Weiterführung der Zertifizierung unter Bedingungen, die von der Zertifizierungsstelle festgelegt werden (z. B. verstärkte Überwachung), erlauben insofern die Verletzung von Zertifizierungskriterien die Anforderungen der zertifizierten Schutzklasse nicht gefährdet und sofortige Abstellmaßnahmen durch den Cloud-Anbieter vorgenommen werden.

(3) Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, unter welchen Aspekten Zweifel an der Einhaltung der Zertifizierungskriterien bestehen (s. EDPB Annex 1 Tz. 7.4).
(4) Stellt die Zertifizierungsstelle die Erforderlichkeit einer Zwischenprüfung fest, so müssen folgende Anforderungen erfüllt werden:

    (a) die Zertifizierungsstelle setzt dem Cloud-Anbieter eine angemessene Frist zur Durchführung der Zwischenprüfung. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden;
    (b) eine angeordnete Zwischenprüfung muss die Anforderungen der Ermittlung, Bewertung und Entscheidung dieses Programms erfüllen (s. ISO/IEC 17065:2012 Tz. 7.11.2, Tz. 7.11.5);
    (c) Werden Auswahl- und Ermittlungstätigkeiten für eine Zwischenprüfung notwendig, können diese durch (ausgegliederte) Evaluatoren durchgeführt werden;
    (d) notwendige Bewertungs- und Entscheidungstätigkeiten müssen von der Zertifizierungsstelle durchgeführt werden. Die Zertifizierungsstelle benennt hierfür Personal, welches die geforderten Kompetenzen unter § 4.2.3 erfüllt (s. ISO/IEC 17065:2012 Tz.7.11.4).

(5) Die Zertifizierungsstelle trifft aufgrund ihrer Feststellungen, ggf. auf der Grundlage des Zwischenprüfungsberichts, die zur Einhaltung des AUDITOR-Kriterienkatalogs erforderlichen Maßnahmen. Hierzu gehören:

    (a) die Zertifizierungsstelle kann die Zertifizierung einschränken (s. § 5.6.5);

(b) die Zertifizierungsstelle kann die Zertifizierung für einen festgelegten Zeitraum vorbehaltlich der Abstellmaßnahmen durch den Cloud-Anbieter aussetzen (s. § 5.6.6);
(c) die Zertifizierungsstelle kann die Zertifizierung widerrufen (s. § 5.6.7).

(6) Die Zertifizierungsstelle gibt dem Cloud-Anbieter vor ihrer Entscheidung Gelegenheit zur Stellungnahme. Die Entscheidung ist zu begründen und dem Cloud-Anbieter in Textform zuzustellen.
(7) Auf Antrag des Cloud-Anbieters kann eine Änderungszertifizierung erfolgen.

§ 5.6.5 Einschränkung der Zertifizierung

(1) Die Zertifizierung kann mit Einschränkungen erteilt oder anstelle eines Widerrufs oder einer Aussetzung der Gültigkeit eingeschränkt werden, wenn zwar die Zertifizierungskriterien für die beantragte Schutzklasse nicht erfüllt sind, aber die Zertifizierungskriterien einer geringeren Schutzklasse erfüllt sind. In diesen Fällen kann die Zertifizierung für eine geringere Schutzklasse erteilt werden.
(2) Der Cloud-Anbieter kann jederzeit die Einschränkung der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem keine schwerwiegenden Gründe entgegenstehen.
(3) Die Einschränkung der Zertifizierung wird drei Wochen nach Zustellung der Entscheidung über die Einschränkung wirksam.
(4) Wenn die Zertifizierung eingeschränkt ist, muss die Zertifizierungsstelle Maßnahmen ergreifen und alle erforderlichen Änderungen an formalen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Konformitätszeichen, usw. vornehmen, um sicherzustellen, dass der eingeschränkte Geltungsbereich der Zertifizierung dem Cloud-Anbieter klar mitgeteilt wird und eindeutig in der Zertifizierungsdokumentation sowie in öffentlichen Informationen beschrieben ist (s. ISO/IEC 17065:2012 Tz. 7.11.3). Hierzu zählen insbesondere die Änderung des Konformitätszeichens sowie die Änderung des Eintrags der Datenverarbeitungsvorgänge in dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.
(5) Die Zertifizierungsstelle stellt sicher, dass der Cloud-Anbieter die Werbung mit der Zertifizierung in Einklang mit der Einschränkung ändert und weitere von der Zertifizierungsstelle definierte Maßnahmen umsetzt.
(6) Die Aufsichtsbehörde ist über die Einschränkung zu informieren (s. EDPB Annex 1 Tz. 7.11).
(7) Die Zertifizierungsstelle fordert den Cloud-Anbieter auf, seine Cloud-Nutzer über die Einschränkung zu informieren.

§ 5.6.6 Aussetzung der Zertifizierung

(1) Eine Aussetzung bezeichnet ein vorübergehendes Außerkraftsetzen der Konformitätsaussage für den gesamten festgelegten Geltungsbereich der Bestätigung oder für Teile davon (s. ISO/IEC 17000:2004 Tz. 6.2).
(2) Der Cloud-Anbieter kann jederzeit die Aussetzung der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem nicht schwerwiegende Gründe entgegenstehen.
(3) Die Zertifizierungsstelle kann die Zertifizierung für die Dauer eines Feststellungsverfahrens aussetzen.
(4) Die Aussetzung wird sofort wirksam.
(5) Wenn die Zertifizierung ausgesetzt wird, muss die Zertifizierungsstelle Maßnahmen ergreifen, um alle erforderlichen Veränderungen an formellen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vornehmen, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass die Datenverarbeitungsvorgänge weiterhin zertifiziert sind (s. ISO/IEC 17065:2012 Tz. 7.11.3). Hierzu zählen insbesondere der Entzug des Konformitätszeichens sowie die Entfernung der Datenverarbeitungsvorgänge aus dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.
(6) Die Zertifizierungsstelle stellt sicher, dass der Cloud-Anbieter die Werbung mit der Zertifizierung einstellt und weitere von der Zertifizierungsstelle definierte Maßnahmen umsetzt.
(7) Wenn die Zertifizierung nach der Aussetzung wieder in Kraft gesetzt wird, muss die Zertifizierungsstelle alle Änderungen an formalen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vornehmen, um sicherzustellen, dass alle entsprechenden Hinweise, dass die Datenverarbeitungsvorgänge weiterhin zertifiziert sind, vorhanden sind (s. ISO/IEC 17065:2012 Tz. 7.11.6). Der Cloud-Anbieter darf dann auch die Werbung mit der Zertifizierung fortsetzen.
(8) Die Datenschutz-Aufsichtsbehörde ist über die Aussetzung zu informieren (s. EDPB Annex 1 Tz. 7.11).

(9) Die Zertifizierungsstelle fordert den Cloud-Anbieter auf, seine Cloud-Nutzer über die Aussetzung zu informieren.

§ 5.6.7 Widerruf der Zertifizierung

(1) Der Widerruf bezeichnet das Zurückziehen der Zertifizierung (s. ISO/IEC 17000:2004 Tz. 6.3).
(2) Der Cloud-Anbieter kann jederzeit den Widerruf der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem keine schwerwiegenden Gründe entgegenstehen.
(3) Die Zertifizierung ist zu widerrufen, wenn

(a) die Zertifizierungsstelle feststellt, dass die Voraussetzungen für die Erteilung der Zertifizierung nicht vorlagen oder nicht mehr vorliegen;
(b) die für den Cloud-Anbieter zuständige Datenschutz-Aufsichtsbehörde feststellt, dass die Voraussetzungen für die Zertifizierung nicht vorliegen oder nicht mehr vorliegen (s. EDPB Annex 1 Tz. 7.11). Der Widerruf erfolgt durch die Zertifizierungsstelle auf Anweisung der zuständigen Datenschutz-Aufsichtsbehörde (Art. 58 Abs. 2 lit. h DSGVO);
(c) wenn eine Zwischenprüfung nicht oder nicht innerhalb der festgelegten Frist durchgeführt wird;
(d) wenn die Akkreditierung der Zertifizierungsstelle ausgesetzt oder widerrufen wird (s. § 4.1.1);
(e) wenn der Programminhaber von AUDITOR feststellt, dass der AUDITOR-Kriterienkatalog die gesetzlichen Vorgaben der Datenschutz-Grundverordnung und des BDSG oder die an deren Stelle tretenden gesetzlichen Bestimmungen nicht oder nicht mehr erfüllt. Dies gilt nicht, wenn der Cloud-Anbieter unverzüglich eine Änderungszertifizierung nach einer neuen Version der AUDITOR-Kriterienkatalogs beantragt und diese unverzüglich durchgeführt wird.

(4) Der Widerruf wird drei Wochen nach Zustellung der Entscheidung über den Widerruf wirksam.
(5) Wenn die Zertifizierung widerrufen wird, muss die Zertifizierungsstelle Maßnahmen ergreifen, um alle erforderlichen Veränderungen an formellen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vornehmen, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass der Datenverarbeitungsvorgang weiterhin zertifiziert ist (s. ISO/IEC 17065:2012 Tz. 7.11.3). Hierzu zählen insbesondere der Entzug des Konformitätszeichens sowie die Entfernung des Datenverarbeitungsvorgangs aus dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.
(6) Die Zertifizierungsstelle stellt sicher, dass der Cloud-Anbieter die Werbung mit der Zertifizierung einstellt und weitere von der Zertifizierungsstelle definierte Maßnahmen umsetzt.
(7) Die Aufsichtsbehörde ist über den Widerruf zu informieren (s. EDPB Annex 1 Tz. 7.8).
(8) Die Zertifizierungsstelle fordert den Cloud-Anbieter auf, seine Cloud-Nutzer über den Widerruf zu informieren.

§ 5.6.8 Erweiterung der Zertifizierung

(1) Der Cloud-Anbieter kann jederzeit die Erweiterung der Zertifizierung beantragen. Die Erweiterung bezeichnet die Erhöhung der Schutzklasse.
(2) Der Cloud-Anbieter muss im Rahmen einer Änderungszertifizierung nachweisen, dass er die Anforderungen der höheren Schutzklasse erfüllt.
(3) Die Zertifizierungsstelle bewertet die Ergebnisse der Änderungszertifizierung und entscheidet über die Vergabe einer Zertifizierung mit höherer Schutzklasse.
(4) Die Anforderungen für Ermittlungs-, Bewertungs-, und Entscheidungstätigkeiten sind auch bei der Änderungsprüfung für eine Erweiterung anzuwenden.

§ 5.6.9 Änderungszertifizierung

(1) Wenn dieses Konformitätsbewertungsprogramm oder der AUDITOR-Kriterienkatalog neue oder überarbeitete Zertifizierungskriterien oder sonstige Anforderungen einführt, die den Cloud-Anbieter betreffen, muss die Zertifizierungsstelle sicherstellen, dass diese Änderungen allen Cloud-Anbietern zur Kenntnis gegeben werden (s. auch § 4.3.5) (s. ISO/IEC 17065:2012 Tz. 7.10.1).
(2) Die Zertifizierungsstelle legt eine angemessene Frist zur Umsetzung der Kriterien oder Anforderungen für einen Cloud-Anbieter fest und informiert diesen darüber. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.

(3) Die Zertifizierungsstelle muss die Umsetzung der Änderungen durch die Cloud-Anbieter überprüfen. Die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist.

(4) Stellt die Zertifizierungsstelle die Erforderlichkeit einer Zwischenprüfung fest, setzt sie dem Cloud-Anbieter eine angemessene Frist zur Durchführung der Zwischenprüfung. Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, unter welchen Aspekten Zweifel an der Einhaltung der Zertifizierungsvoraussetzungen bestehen. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.

(5) Die Zertifizierungsstelle kann die Zertifizierung für die Dauer der Änderungszertifizierung aussetzen (s. § 5.6.6).

(6) Die Zertifizierungsstelle trifft aufgrund ihrer Feststellungen, ggf. auf der Grundlage des Zwischenprüfungsberichts, die zur Einhaltung des AUDITOR-Kriterienkatalogs erforderlichen Maßnahmen. Sie kann die Zertifizierung als weiterhin gültig kennzeichnen, einschränken, aussetzen oder widerrufen. Die Zertifizierungsstelle gibt dem Cloud-Anbieter vor ihrer Entscheidung Gelegenheit zur Stellungnahme. Die Entscheidung ist zu begründen und dem Cloud-Anbieter in Textform zuzustellen.

(7) Die Zertifizierungsstelle muss sonstige Änderungen berücksichtigen, welche die Zertifizierung beeinflussen können, einschließlich Änderungen, die durch den Cloud-Anbieter ausgelöst werden, und über die geeigneten Maßnahmen entscheiden (s. ISO/IEC 17065:2012 Tz. 7.10.2). Hierzu zählen insbesondere:

   (a) Veränderungen an zertifizierten Datenverarbeitungsvorgängen des Cloud-Anbieters gemäß § 4.3.3;
   (b) Veränderungen im regulatorischen und IT-Umfeld von Cloud-Diensten, darunter bspw. die Bekanntmachung von neuen Sicherheitslücken und Schwachstellen, oder die Aktualisierung des Stands der Technik (s. auch § 4.3.5 und § 4.3.4);
   (c) die Bekanntmachung, dass bisherige Sicherheitsmaßnahmen als unzureichend oder unsicher eingestuft werden, bspw. die Verwendung von veralteten Verschlüsselungsverfahren.

6 Anhang A: Festlegung der Ermittlungszeit

6.1 Allgemeines

6.1.1 Grundlagen

Die Zertifizierungsstelle muss dokumentierte Verfahren zur Festlegung des Ermittlungszeitaufwands haben (s. ISO/IEC 17065:2013 Tz. 7.4.1). Für jeden Cloud-Anbieter muss der Zeitaufwand, der benötigt wird, um eine vollständige und wirksame Ermittlung planen und durchführen zu können, individuell ermittelt werden. Grundsätzlich muss die Ermittlungszeit gering sein, um auch die Zertifizierung von kleinen und mittelständigen Cloud-Anbietern zu ermöglichen (i.S.d. Art. 42 Abs. 1 DSGVO). Gleichzeitig müssen ein möglichst hoher Prüfumfang und eine ausreichende Prüftiefe erreicht werden, um die die Schutzaussage der AUDITOR-Zertifizierung und die Einhaltung der Anforderungen der Datenschutz-Grundverordnung sicherzustellen. Im Folgenden werden daher grundlegende Konzepte zur Festlegung des Ermittlungsaufwands festgelegt, welche einen vergleichbaren Ermittlungszeitaufwand definieren und möglichst zur budgetären Planungssicherheit bei Cloud-Anbietern und Zertifizierungsstelle beitragen sollen.

6.1.2 Verteilung des Zeitaufwands

Die Ermittlungszeit schließt die Vor-Ort-Zeit in den Räumlichkeiten des Cloud-Anbieters ein sowie die Zeit, die außerhalb des Geländes zur Durchführung der Planung, Dokumentenprüfung, Kommunikation mit dem Personal des Cloud-Anbieters und zum Verfassen des Ermittlungsberichts aufgewendet wird (s. IAF MD 5:2015 Tz. 2.1). Ein Ermittlungstag umfasst in der Regel 8 Stunden. Reisen (An-, Abreise oder zwischen Standorten) sowie jegliche Unterbrechung sind nicht in die Ermittlungszeit eingeschlossen. Die aufgewendete Zeit der Teammitglieder, die nicht als Evaluator eingesetzt sind (bspw. Fachexperten, Übersetzer, Dolmetscher, Beobachter und Auditoren in Ausbildung), darf nicht zu dem festgelegten Ermittlungszeitaufwand gezählt werden.

Der geplante Ermittlungszeitaufwand sollte sich in die Aspekte „Projekt-Overhead und Dokumentenprüfung“ mit ca. 35% (dazu gehören bspw. Aufwände für Planung und Berichterstattung) und die „Detailermittlung“ mit ca. 65% des Gesamtaufwands aufteilen. Bei der Detailermittlung werden vor allem Ermittlungen vor Ort durchgeführt. Wenn Remote-Techniken wie Web-Meetings, Telefonkonferenzen oder elektronische Fernprüfung der Datenverarbeitungsvorgänge (bspw. Penetrationstests oder Schwachstellenanalysen) verwendet werden, sollten diese Aktivitäten im Ermittlungsplan (s. § 5.2.2) aufgeführt werden und können als Teil der gesamten „Detailermittlung“ betrachtet werden. Fernprüfungen dürfen jedoch nur bei begründeten Ausfällen mehr als 30% der geplanten Ermittlungszeit vor Ort ausmachen. Ist für die Planung und/oder Erstellung von Berichten zusätzliche Zeit erforderlich, so ist dies keine Rechtfertigung für die Verkürzung der Ermittlungszeit vor Ort.

Die jährlich für Überwachungen aufgewendete Gesamtzeit sollte etwa ein Drittel der Ermittlungszeit betragen, die für die Erstzertifizierungsprüfung aufgewendet wurde (s. IAF MD 5:2015 Tz. 5, und § 5.6.2). Die geplante Überwachungszeit sollte von Zeit zu Zeit überprüft werden, um Änderungen zu berücksichtigen, die sich auf die Überwachungszeit auswirken.

Zur Gewährleistung der Effektivität der Ermittlung, sollte die Zertifizierungsstelle auch die Zusammensetzung und Größe des Ermittlungsteams berücksichtigen (z.B.: ½ Tag mit 2 Evaluatoren ist ggf. weniger effektiv, wie 1 Tag mit 1 Evaluator; oder 1 Tag mit einen Leitenden Evaluator und einem Experten ist effektiver als 1 Tag ohne den Experten) (s. IAF MD 5:2015 Tz. 2.2.4).

6.2 Berechnung der Ermittlungszeit

6.2.1 Faktoren bei der Berechnung der Ermittlungszeit

Zur Berechnung der Ermittlungszeit sind folgende zwei (ggf. gegenseitig abhängige) Faktoren maßgeblich:

1) Anzahl der Mitarbeiter, welche an Erbringung des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge mitwirken. Dieser Faktor ist maßgeblich, unter anderem da die Kompetenz, die Bekanntheit der Richtlinien und Anweisungen sowie die korrekte Ausführung von organisatorischen Prozessen überprüft werden muss. Zudem ist die Anzahl der Mitarbeiter ein Indikator für das Ausmaß der Datenverarbeitung.
2) Anzahl der Cloud-Nutzer, welche den Cloud-Dienst beziehen. Wird der Cloud-Dienst durch eine steigende Zahl von Nutzern genutzt, so sind nicht nur mehr Bestands- und Nutzungsdaten vorhanden, die einen besonderen Schutz bedürfen (s. Kapitel VII des AUDITOR-Kriterienkatalogs), sondern auch die Anzahl der Betroffenen steigt tendenziell an. Darüber hinaus

steigt bspw. die Anzahl an zu prüfenden rechtsverbindlichen Vereinbarungen und der Umfang an Vorkehrungen zur Wahrung der Betroffenenrechte.

Darüber hinaus sollte bei der Feststellung des Ermittlungszeitaufwandes weitere und Cloud-Dienst-spezifische Aspekte berücksichtigen. Dazu zählen unter anderem:

(1) Komplexität des Cloud-Anbieters und des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge;
(2) beantragte Schutz- und Wiederherstellbarkeitsklasse;
(3) Anzahl der Standorte, deren geographische Lage sowie Erwägungen zu Mehrfach-Standorten;
(4) technologischer und organisatorischer Kontext, darunter
  (a) der TOM des Cloud-Anbieters i.S.d. Art. 28 DSGVO;
  (b) eingesetzte Technik und IT-Landschaft, dazu zählen insbesondere relevante IT-Systeme;
  (c) organisatorische Prozesse zur Durchführung der Datenverarbeitungsvorgänge;
  (d) ausgegliederte Entwicklungsarbeiten;
(5) Verschachtelung der Cloud-Lieferkette, ausgegliederte Vorgänge und Schnittstellen zu Subauftragsverarbeitern;
(6) spezifische Datenschutzrisiken des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge.

6.2.2 Ermittlungszeitdiagramm

Das nachstehende Ermittlungszeitdiagramm gibt den Ausgangspunkt für eine durchschnittliche Anzahl von Ermittlungstagen an. Das Diagramm bietet daher einen Rahmen für die Ermittlungsplanung, indem es einen Ausgangspunkt auf der Grundlage der Gesamtzahl der Mitarbeiter und Anzahl der Cloud-Nutzer für alle Schutzklassen ermittelt. Dieses Zeitdiagramm ist unter Berücksichtigung der Faktoren zur Anpassung der Ermittlungszeit und Einschränkungen der maximalen Abweichung zu verwenden (s. 6.2.3 und 6.2.4 unten). Das Ermittlungszeitdiagramm unterteilt die Ermittlungstage auch anhand der Schutzklassen, wobei eine Erhöhung um 10% für Schutzklasse 2 und eine Erhöhung um 20% für Schutzklasse 3, aufgerundet auf den nächst höheren Tag, im Vergleich zu den Ermittlungstagen für Schutzklasse 1 angenommen wird.

Die Zertifizierungsstelle betrachtet dabei alle zwei Faktoren (Anzahl Mitarbeiter, Anzahl Cloud-Kunden), insofern Informationen hierzu vorliegen, und wählt die Ermittlungstage, welche die meisten unter allen zwei Faktoren sind. Beispielsweise wird im Rahmen einer Ermittlungsplanung festgestellt, dass 14 Mitarbeiter beim Cloud-Anbieter arbeiten und 10 Cloud-Kunden den Dienst nutzen. Für Schutzklasse 2 ergeben sich daher im Durchschnitt 7 Ermittlungstage, da die Anzahl der Mitarbeiter in diesem Falle maßgeblich für die Festlegung der meisten Ermittlungstage ist.

Anzahl Mitarbeiter	Anzahl Cloud-Kunden	Zeitaufwand je Schutzklasse (SK) in Ermittlungstagen		
		SK 1	SK 2	SK 3
1~10	1~10	5	6	6
11~15	11~25	6	7	8
16~25	26~50	7	8	9
26~45	51~100	8,5	10	11
46~65	101~150	10	11	12
66~85	151~250	11	13	14
86~125	251~500	12	14	15
126~175	501~1000	13	15	16
176~275	1.001~1.750	14	16	17
276~425	1.751~3.000	15	17	18
426~625	3.001~5.000	16,5	19	20
626~875	5.001~10.000	17,5	20	21
876~1.175	10.000~17.500	18,5	21	23
1.176~1.550	17.501~25.000	20	22	24
> 1.550	> 25.000	Folgt dem Fortschritt oben	Folgt dem Fortschritt oben	Folgt dem Fortschritt oben

6.2.3 Faktoren für die Anpassung der Ermittlungszeit

Das Ermittlungszeitdiagramm darf nicht isoliert verwendet werden. Die Zertifizierungsstelle muss weitere Faktoren berücksichtigen, die einerseits zusätzliche Ermittlungszeit erfordern, oder andererseits zu einer Verringerung der Ermittlungszeit führen.

Beispielfaktoren, die eine Ermittlungszeit verlängern, sind:

- Wiederherstellbarkeitsklasse 2 erfordert in der Regel eine zusätzliche Zeit von 0,25 Ermittlungstagen.
- Wiederherstellbarkeitsklasse 3 erfordert in der Regel eine zusätzliche Zeit von 0,5 Ermittlungstagen.
- Ermittlung bei mehreren Standorten (z.B. mehrere Rechenzentren oder ausgelagerte Entwicklungsteams; s. § 5.2.6).
- Der Verarbeitungsvorgang deckt hoch komplexe Verfahren oder eine relativ große Zahl einzigartiger Aktivitäten ab.
- Mitarbeiter, die mehr als eine Sprache sprechen (die einen oder mehrere Dolmetscher erfordern oder einzelne Evaluatoren daran hindern, unabhängig zu arbeiten) oder Unterlagen, die in mehr als einer Sprache vorgelegt werden.
- Es ist eine Vielzahl von Funktionen oder Prozesse ausgegliedert bzw. eine Vielzahl von Subauftragsverarbeitern wird eingesetzt.
- Es liegen Beschwerden aus der Vergangenheit vor oder Überwachungsergebnisse oder bisherige Erfahrungen mit dem Datenverarbeitungsvorgang lassen erhöhten Ermittlungsbedarf erwarten.

Beispiele für Faktoren, die eine kürzere Ermittlungszeit ermöglichen, sind:

- Geringe Datenschutzrisiken der Datenverarbeitung (bspw. Aufgrund angewendeter Pseudonymisierungs- und Anonymisierungsverfahren) oder Tätigkeiten geringer Komplexität.
- hoher Prozentsatz von Personen, die unter der Kontrolle des Cloud-Anbieters arbeiten und dieselben Aufgaben erfüllen.
- Vorkenntnisse und hohe Bereitschaft des Cloud-Anbieters (z.B. wenn der Cloud-Anbieter bereits von derselben Zertifizierungsstelle nach einer anderen Norm zertifiziert wurde).
- Anerkennung von bestehenden Zertifikaten (s. § 5.1.7), sodass nur eine stichprobenartige Ermittlung bei einer Vielzahl von Kriterien von Nöten ist.
- Eine Vielzahl von Kriterien sind nicht anwendbar für den Zertifizierungsgegenstand (s. § 5.1.5).
- Sehr kleiner Standort im Verhältnis zur Anzahl der Mitarbeiter (z. B. nur ein Bürokomplex).
- Hoher Automatisierungsgrad.

Verlängernde Faktoren können durch verkürzende Faktoren ausgeglichen werden. Die im Ergebnis der Berechnung erhaltene Dezimalzahl sollte auf den nächst halben Tag auf- bzw. abgerundet werden (z.B. aus 5,3 Ermittlungstage werden 5,5 Ermittlungstage; aus 5,2 Ermittlungstage werden 5 Ermittlungstage; s. IAF MD5:2015 Tz. 2.2.3).

6.1.3 Begrenzung der Abweichung der Ermittlungszeit

Um eine wirksame Durchführung der Ermittlung zu gewährleisten und zuverlässige und vergleichbare Ergebnisse zu gewährleisten, darf die im Ermittlungszeitplan angegebene Ermittlungszeit nicht um mehr als 30% verkürzt werden.

In allen Fällen, in denen Anpassungen an der im Ermittlungszeit vorgesehenen Zeit vorgenommen werden, sind ausreichende Nachweise (inkl. Begründungen für Abweichungen) und Aufzeichnungen aufzubewahren, um die Änderung zu rechtfertigen. Die Zertifizierungsstelle soll sicherstellen, dass jegliche Veränderungen in der Ermittlungszeit nicht zu einer Gefährdung der Wirksamkeit der Zertifizierung führen.

Die Zertifizierungsstelle berichtet jährlich an den Programmeigner, welche Ermittlungszeiten für die Zertifizierung veranschlagt und abgerechnet wurden (s. § 4.4.4). Auf Rückfrage des Programmeigners stellt die Zertifizierungsstelle die Begründung hierfür zur Verfügung.

7 Referenzen

Beschluss Nr. 768/2008/EG	Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates (Text von Bedeutung für den EWR); http://data.europa.eu/eli/dec/2008/768(1)/oj
DAkkS 71 SD 0 001	Allgemeine Regeln zur Akkreditierung von Konformitätsbewertungsstellen. Revision: 1.3 | 29. August 2012
DAkkS 71 SD 0 013	Festlegungen für die Anwendung der DIN EN ISO/IEC 17065 bei der Akkreditierung von Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Revision: 1.1 | 04. Dezember 2014
DAkkS 71 SD 0 016	Regel zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme gemäß Tz. 4.6.3 EN ISO/IEC 17011. Revision: 1.3 | 27.11.2018
DSK	Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065. Version 1.2 (21.01.2020). Vorläufige Fassung
EDPB Annex 1	EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1. Version 3.0 Stand 04.06.2019
IAF MD 2:2017	Verbindliches Dokument für die Übertragung akkreditierter Zertifizierungen von Managementsystemen. (Deutsche Übersetzung des IAF Dokumentes „IAF MD 2:2017“); https://www.dakks.de/sites/default/files/dokumente/iaf_md_2-2017_verbindliches_dokument_fuer_die_uebertragung_akkreditierter_zertifizierungen_von_managementsystemen_uebersetzung_20190826_v1.0_0.pdf
IAF MD 4:2018	IAF MANDATORY DOCUMENT FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) FOR AUDITING/ASSESSMENT PURPOSES Issue 2. Stand 2018
IAF MD 5:2015	Ermittlung von Auditzeiten für die Auditierung von Qualitäts- management- (QMS) und Umweltmanagementsystemen (UMS). (Deutsche Übersetzung des IAF Dokumentes „IAF MD 5:2015“); https://www.dakks.de/sites/default/files/dokumente/71_sd_6_021_iaf_md_5-2015_auditzeiten_qms_ums_20160331_v1.4_0.pdf. Stand 13. März 2016
IAF MD 1:2018	Verbindliches IAF Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten (Deutsche Übersetzung des IAF Dokumentes „IAF MD 1:2018“); https://www.dakks.de/sites/default/files/dokumente/iaf_md_1-2018_auditierung_und_zertifizierung_von_managementsystemen_in_organisationen_mit_mehreren_standorten_uebersetzung_20181218_v1.0.pdf. Stand 29. Januar 2018
IAF/ILAC A5:11/2013	IAF/ILAC Multi-Lateral Mutual Recognition Arrangements (Arrangements): Application of ISO/IEC 17011:2004. Stand 2013
ISO/IEC 15408:2009	Information technology -- Security techniques -- Evaluation criteria for IT security. Stand 2009
ISO/IEC 17000:2004	Begriffe und allgemeine Grundlagen. Stand 2004.
ISO/IEC 17011:2017	Allgemeine Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren. Stand 2017
ISO/IEC 17020:2012	Anforderungen an den Betrieb verschiedener Typen von Stellen, die Inspektionen durchführen. Stand 2012
ISO/IEC 17021-1:2015	Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen. Stand 2015
ISO/IEC 17024:2012	Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren. Stand 2012
ISO/IEC 17025:2017	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien. Stand 2017
ISO/IEC 17030:2009	Allgemeine Anforderungen an Konformitätszeichen einer dritten Seite. Stand 2009

ISO/IEC 17040:2005	Konformitätsbewertung - Allgemeine Anforderungen an die Begutachtung unter gleichrangigen Konformitätsbewertungsstellen und Akkreditierungsstellen. Stand 2005
ISO/IEC 17065:2012	Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Stand 2012
ISO/IEC 17067:2013	Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme. Stand 2013
ISO/IEC 18045:2008-018	Information technology -- Security techniques -- Methodology for IT security evaluation. Stand 2008
ISO 19011:2018	Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018). Stand 2018
Lins et al. (2016)	Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic Certification of Cloud Services: Trust, but Verify! IEEE Security and Privacy, 14(2), 67–71. https://doi.org/10.1109/MSP.2016.26
Lins et al. (2019)	Lins, S., Schneider, S., Szefer, J., Ibraheem, S., & Sunyaev, A. (2019). Designing Monitoring Systems for Continuous Certification of Cloud Services: Deriving Meta-requirements and Design Guidelines. Communications of the Association for Information Systems, 44. https://doi.org/10.17705/1CAIS.04425
Merkblatt zu Akkreditierungsverfahren im Datenschutz	Merkblatt zu Akkreditierungsverfahren im Datenschutz. Stand 13.03.2020. https://www.dakks.de/content/merkblatt-zu-akkreditierungsverfahren-im-datenschutz
NIST (2011)	Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing. https://csrc.nist.gov/publications/detail/sp/800-145/final